Software Engineering Institute
Carnegie Mellon University

1999 CERT Advisories

CERT Division

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the

SEI Administrative Agent
AFLCMC/AZS
5 Eglin Street
Hanscom AFB, MA 01731-2100

DM17-0052

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Table of Contents

1 CA-1999-01: Trojan horse version of TCP Wrappers

Original issue date: January 21, 1999
Last revised: January 22, 1999

A complete revision history is at the end of this file.

The original release of this advisory contained an error. Please take note of the changes mentioned in the revision history section at the end of this file.

The CERT Coordination Center has received confirmation that some copies of the source code for the TCP Wrappers tool (tcpd) were modified by an intruder and contain a Trojan horse.

We strongly encourage sites running the TCP Wrappers tool to immediately verify the integrity of their distribution.

I. Description

TCP Wrappers is a tool commonly used on Unix systems to monitor and filter connections to network services.

The CERT Coordination Center has received confirmation that some copies of the file tcp_wrappers_7.6.tar.gz have been modified by an intruder and contain a Trojan horse. This file contains the source code for TCP Wrappers version 7.6. This Trojan horse appears to have been made available on a number of FTP servers since Thursday, January 21, 1999 at 06:16:00 GMT. Copies downloaded prior to this time are not affected by this particular trojan horse.

The Trojan horse version of TCP Wrappers provides root access to intruders initiating connections which have a source port of 421. Additionally, upon compilation, this Trojan horse version sends email to an external address. This email includes information identifying the site and the account that compiled the program. Specifically, the program sends information obtained from running the commands 'whoami' and 'uname -a'.

II. Impact

An intruder can gain unauthorized root access to any host running this Trojan horse version of TCP Wrappers.

Note: If you have already installed a Trojan horse version of TCP Wrappers, intruders can identify your site using information contained in this advisory. Please read the "Solution" section and take appropriate action to protect your site as soon as possible.

III. Solution

We encourage sites who downloaded a copy of the TCP Wrapper after Thursday, January 21, 1999 at 06:16:00 GMT to verify the authenticity of their TCP Wrapper distribution, regardless of where it was obtained.

You can use the following MD5 checksums to verify the integrity of your TCP Wrappers distribution:

```
Correct version:

    tcp_wrappers_7.6.tar.gz

        MD5  = e6fa25f71226d090f34de3f6b122fb5a

        size = 99438

    tcp_wrappers_7.6.tar

        MD5  = 5da85a422a30045a62da165404575d8e

        size = 360448

Trojan Horse version:

    tcp_wrappers_7.6.tar.gz

        MD5  = af7f76fb9960a95a1341c1777b48f1df

        size = 99186
```

Appendix A provides checksums for the individual files within the distribution.

It is not sufficient to rely on the timestamps of the file when trying to determine whether or not you have a copy of the Trojan horse version.

Additionally, the file tcp_wrappers_7.6.tar.gz is distributed with the detached PGP signature tcp_wrappers_7.6.tar.gz.sig.

Wietse Venema is the author and maintainer of the TCP Wrappers distribution.You can verify the integrity and authenticity of your distribution with Wietse Venema's PGP public key. We have included a copy of his PGP public key below. Note that the Trojan horse version was not signed, and that Wietse Venema's PGP key was not compromised in any way.

As a workaround, until you are able to verify your copies of TCP Wrappers, you can block inbound connections with a source port of 421 at your network perimeter. However, it is possible that some operating systems or software may use port 421 in legitimate connections. Thus, it is possible that some legitimate connections might be blocked.

Where to Get TCP Wrappers

Wietse Venema has moved the primary FTP archive for TCP Wrapper source to a different location. The primary archive is now located at ftp://ftp.porcupine.org/pub/security/.

Sites that mirror the TCP Wrapper source code are encouraged to update their mirroring procedures.

Wietse Venema expresses his gratitude to his former employer, Eindhoven University, for making possible the development and distribution of the TCP Wrapper software, and appreciates the support from system administrators of the department of mathematics and computing science.

Additionally, we have verified that the distribution of TCP Wrappers offered by the CERT Coordination Center at ftp.cert.org was not involved in this activity. TCP Wrappers is available from our FTP site at ftp://ftp.cert.org/pub/tools/tcp_wrappers/tcp_wrappers_7.6.tar.gz.

MD5 checksum: e6fa25f71226d090f34de3f6b122fb5a

Wietse Venema's PGP Public Key

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6.2

mQCNAirDhV8AAAED/i4LrhQ/mwOgam8ZfQpEcxYoE9kru5oRDGtoVeKae/4bUver

aGX7qVtskD6vwPwr2FF6JW2c+z2oY4JGPGUArORiigoT82/q6vqT0Wm1jIPsXQSB

ZCkBoyvBcmXEi+J7eDBbWLPDxeDimgrORbAIQ4uikRafs8KlpNyA8qbVMny5AAUR

tCV3aWV0c2UgdmVuZW1hIDx3aWV0c2VAd3p2Lndpbi50dWUubmw+iQEVAwUQNEfn

hgyPsuGbHvEpAQExUAgAkAZTAVqzICTlVMggjsG9NghqC0FPqO2s9BQLXH3lQDdQ

C2tOx1CYvL3pB8X77alh18/HnUd6PNkloHC2fqNo5eNyuVDeUpvW+mz6IRlndnJU

kLVx/Kzu+h3TooWlX/BSc+k0XsQJ7mpP4QeWvoHll50rBPVLYnv4ODbZh0z5jYfr

Yq2n/05vi5nRdz2gXqRRIorfD46a5n+gQNAvrwhKMRZeyqEfOCtQ+UjMH7tyGG0N

+suzNQtBjypEZkB8OFEQB1Q3RatQlWx55JOfmcba0JBY9umOuNoDPldvIgMbExRP

5tN+qOjsHbm723S1kybyQKEbQgx3pDA3xiz9SBFqjYkBFQMFEDRH59NGYudYIBG4

eQEB3XMH/RXG4wFjy32JDJPaVmS14Ax53VGOBUDLZo9Uv8lG3uTIe886lLeDqWA2

fHyyUFwUBC917NR0D9HCTAAQ5PZYO7kOV5JMSLWoxyLYRimHcUnhfBJ9XthVvjvH

NuItWWXVLND0UjTkmHJSCtTxcM6Yo7NuisIJOYcnRameWK105FPb9i3ATaEejM8C

NPfgiHp9Krv5EVfAHJ+gBy/q4kKqQYFZgdbogVS5aKQJiO5imGEtxGl7qSxfC1WJ
```

TmrauU/8CbBQM6MvifnIep+LI+IBLwDFSByZDPR5dakjeCGMnNtj2XYEu0mWtz/5
DHOIDGz9whNF1DBUBbHM3BEuUai87eWJAD8DBRA0R+e9YVgWxTrOVf4RAtpXAKDK
jQQ4a7pxrgLA63H4XHhfCNC9PACghwiSLYqPdnsyMM+LN/I3su2zF7OJAJUDBRA0
R+f8d6a8PicAdv0BAXNeBACgGcN9znLn0yHysY852uUntwMS9CAlTdSLkiRaf1gM
sV+VQipFvSzS+rmg/DtiWDJ46Z5ffJe6rMnIn59yGgmkelj6hTDi3eGcarGnIFQJ
PG61JmfdTxtyQ5lY5zpNoBnKwVHCYBoMvpvoe0axVhQm23+j/qll44jcnORmqcYD
YIkAPwMFEDRH56iWgad8PVLgfxECrc8An2xiSfGbEsocbX5eOUkTc6jYiRwCAKDC
FIaSRaNnmB3sHPaj0TnaGri6h4kAlQMFEDRgoatWKpzSj2i9yQEBKQkD/0Znfn9u
jEPIpUpPLO1HvFX16IMx+JXYQcFakporAmvNzw28a351cWNQOTSr0ZS+8G6YNXEQ
WUeI2NE96gIpUmb6m2XNJ5ucdLRG2PsSwwcYtuipRXaR3aHrLwPRDEdlo0ifC+Bm
mV80LrTsnCfR1XvuCGcFkA//BNnXYJnjM36EiQEVAwUQNEUD2zw9PaeQSTXpAQGX
gQgAhlqfuv/aWGeP9Qgdtlq688sP9fADmwzQdQ98lbOL184eW7Or+Dunynh89Sn0
yC90AfwiI3/E75YIZJA4x6qjMan+3p8mNw8WtkUWYZOQ/A91tXQflo/EFqliR4mx
HKmWqubsXzIL6fW3vxC/gQnlNKE3Rx53vwxMMK8u3LFDdLQu0OpXOkmAa4qZh+Pi
DXa77DPYToHcxXeOIvAm+mSqxuBK9URKlGDq4snS3XnlmfdySz2oEsFPN5MUOvQV
gyeHl7aRysa/C8d7tq+FLWN8fQcLpn/3hXHUygdW4KogGVUDFMpckLv1E161AT84
R+fK9ztWoi85CSkFwCESiO8vj4kAlQIFEDBqt5TZp9pcfgqygQEBWvYEAK7oHPhv
4ChPzquWue9maG22iOBO+mJJ6ReKriydzcUUzwwLAEDnzN7TJaWBj7f/M6anrTqT
UxJWcm5R3BzSPecLmM9FN1B+zsJjhqA/BbTjfr7lDuWzplLI55SlezHrSD2Zdh7f
NZp6LjoLWhApUCtwY5JqofYEVutSHLjKnKwAiQEVAwUQMQ6i0ee7tRpdDUB5AQGA
Hgf+MXxcTTo73zq7Iy3n23JjkRYuGRScRyxHPrM4CvCfpxGZ0KqXFydkGjaV2NxW
BUdjZzzrXqExTv/w6l/b/TG5WDqOSkSmmIYYc1c1oaKvbPpwimkzREK9QZABibK8
OA+TN8E2Or7v8/DuwWRVfDdmhblf98PH29wAYvNAwGlftnzfsdOILTxHySZ0724Q
YWDHM876sJ7lvzZ1sPUkv61blq1etB0VrRUJ0YewaqhP/Jmn45ldHRdxjzN8yrzq
u4rzrHx1LJb6j/mHSH7soEwEKpHRCtZNY+PtLcKheFxiFweu8OAMsm574wmybEGr
2EICSA0p4I6UswT0Rcn7Oba/1YkAlQMFEDEOojNOQewbPzG6VQEBXkoEAIoRVBm5
/LmOiOyeB+968KyOPVxCXHZqKePwjt32sz/ozKQUfjvxGE1x2G9gAdSFlfI3qjL3
Iw8MPYspX10nUYbtvcT4QBci6vd/gAut6d1pwl/Rz/ui0HqbjvBxEzLFKNm3ssIp

/FeNyBBO8KZFd+h4Yqc4TqkjiYOnR6CcatI6iQCVAwUQMHjnn+Tyai8iNKttAQHS
IQP+L5lquZYfWQfcYjS+NTTCXC8fSolynnsJfy589knPeQOjxKPv9IdU0bXXzRPh
wXoCftxm08/qrFEzRmLJX8Nbs4VVcJHt1VnoIo+Fu0ASn6JV0f0HiDhPWCJerBYl
wrqTYoPEC8hWGQr93ARda4O83KZ6QQqBFXuKgYHxvHnTTMGJAJUDBRAwc68SAk+E
axRt4o0BAZSCA/9bYDgwudU+uFf2/e2GAUT1gxTHhSPgSKlg8Ca8p6AJeaqB3YvJ
wBgFaqYNNOm0XGl4K2uWXJURTA8rboS+UrN7+besnbLpUZ3WnxIWPMhU0eK4x67M
SH2tSrtz0fZtnOpIkZ0FvPMC/W4yidnGgwT3hxbHjznFH7FE3GYOvWyM/okAlQMF
EDBvvvQx/7eDRBO2kQEBBZwD/jlqZbO1LjpueWSMijLF3ntCm617IcEfG6xz0oRM
M2GEBtgtIIrv5YaTLy8jYPyu5edvvyc/sfcuFBw33wzxThuCfUIqzS/TwjgqSoaT
L1+Rl3h4g+VTSteSWg/+fCfAp5T50DH1Uq3JqiV9lzwdgTK5uMvYmwG8ZHln6ju2
F2E4iQCVAwUQMGqp+hrbNNwC+IyBAQHKggQAtoLHXDwYB2aPM4W3VGdBkT4jm8o1
XgvqaFv/X+7xZKF9UgWRPRFqF88WeZRA2mZb/DxrmuckFsvqhJuvjEvKbr93QYuX
dZG/e7am71WXLBKSPnvsoJY51eT7XrDI6hmqvWcYbngHpHzY+ZB6N9h7qcGw1zRw
t4/Kxbp6nxlFAeqJAJUDBRAwal9L6CVK4w9Ml3UBAY4sBADTn9fOYlwC7iVJVd/z
GMZyW5gvif9PKw+Grfn8S02x9i1OlqX1cgxJkMWoXpQCilQ4jyStv3LekhJ2Btp5
kUCiColOZO4NOb7n0Iuwsnx1TkLl75RWZKDc+7gxA5PxCnzFE+y8O6i4pSuzzhpF
qz4cEnRQ4D+Klrqu+3p43rfETYkAlQIFEDBoJ+kiUZbZZm0AUQEBpNkD/jEfKwJV
xoFTakdUkIyprrZg3uYBTbhwf0rSynUVjm+X3KCbKROEyx6GskzH09D0LT+gTi9z
Z9RrzXv1/yeO/6wte1WZT+vNLhvGrO4yniYm+Os5zSa+5aW/fyHilE02ZNk20r+H
hY6aOmZQ8UXGv+U5ryg48UuGfe920UndQiuYiQCVAwUQMGnKYLnzJzdsy3QZAQGz
lAQAuIRJhf8sAkuy3PeT9UuXvt1uUHwTiEkrDdbFnBQOfmkVxcQOP82gzgWYk5ii
wlTmgT4euodekIzMrMIxqQsqyhvwxxbtD+k3aHFtocrvRUTShO51g8fiQcN7CTbE
eTa3azUpMbiOWnvFTOKqfgAGn039smgkFIojywX7NdE+g+GJAJUDBRAwacpBYmX6
SAdWdFUBAT1dBACeuV567rcGe4rE3Bjl629lWr57C9NtHOfKh63KT1xUHM6f0elq
IfMWBCXTNAmS/rpQ7bjg7+WbWYYct2YKSizpP9/eyFq0Ax2cFzCBi8c2DdUuszEy
PdvX6ZSvXMkR5Z90bLbeH26yzacnyF1MdD0wtAqdtOcs6xHCrfyKl/7CmIkAlQMF
EDBpx1AEJn15jgpJ0QEBCUcD/0gEX5BCjysfVNjRHLibxwv46aqFGf4FED/ZyJEb
jC6szt0q2jzOGZUhMsyYNqmoCSdj2mGDd2AG01HxJRqVpkvaMv5O4XYOvC9oQTwv

8+5EV0Be2HZ+Jfl9Xpyl7TG+3ClQXpUH21C5suiWOTEsexq7a3YvdULELqtlQpBo
pianiQCVAwUQMGf966NsRd57vOpJAQF8ngP9GTFx5J+57n9SsISC/32GleMy0g3l
HJTrjtWnxIOt28DTXI9VxOmaRIh002PJG8d2esFq17DXxJf60M43s14F/6ct/PmB
2psgIayaW+1Mj1FtBAUr4cKsfGZytcKqrHoMvSp7rZHhfgVy/xLMKKCmm+c7xdYJ
Sgbicrpwq1IBuDGJAJUDBRAwZ/wvO3/HvM52ax8BAR+WA/47Zw6LyUQHR0HqikBZ
mu1vTfgG6seat/93V8z2kA80f++FbKisJwzqxUzJ27ERFAgOdbTPGWwuCeWkszd7
TSBVzfoAosU//H1cbIULmD9jv7DLh6lQx+RUEdlD7zkUiVkmhU234AjnzWx1dfLi
g5iJomAE1qLskvbi1k5TRI3St4kAlQMFEDBmoqxYl6t82lyyQQEBekIEANKfx56q
zeVCa9eIic4j2FXpJC5nYUOcdShPkhKWpDZMxNHT5S/gyqZFtgMvqbqKcDsxmtsF
jpHJr7QX1lKBYTAzGUtSPOgb2BiJbHwHfK3GH6TfKqNHt9rYERvBbaekyEEBS8Ds
Vcw1ZTgi/gIBSN83NkLJuc09i/nHg939hdr3iQB1AgUQL8wq2mgPK9CjLmKhAQFv
1AL/bL+vtlG61Dtmu8/kv5HkPiOVqfiomUYI1OfF0amJUNKgBadhdbJ40QGMuhhX
HlWyb4/MnSt4aujnwA8sKhtRKtJHKvjjLf+LTmdMol2wnoK072lLpFumX7aJ3pS1
4aUgiQCVAwUQL4l3ERPcEwSgd4ahAQFt+gP/Zsee/uKXvtMxG5DSCgKpnU9p9QGV
4gnP9bCydQ+brmepEuMSuj9c/VFzHlYLXpJs9ZhfCbjNuuVRyjQIVj3Jbq9s4Xwy
hxc+Q0xglMUhjm18ycJ8PPgkx4e8FdzcSuZfaFI6hH0Er7Jeh/8HOyrKSlsqrGZO
y0HGAuKOWQKP+ZCJAJUDBRAviBbrym8rg/wMAtUBAaEvA/0ZlxCa1Ka/6BQMxaMz
+xdbDPdcbcntpcyuERm2FMY5a2bOr1j4Rpic3zc1+Q9N6ZQA5FJOpWvHB0xXUw5b
No6aG1VAHrmV51jmIUYVJy+DTmXZela9nGHfiM33RvdttDsvox6HTe/teo+fzP3s
6MQaWScLDx33RezVTmVSBk22WYkAlQMFEC99GmfcgPKm1TJ8uQEBJzsD+waYQmJK
G0btGU0+GUTg+bRMSfCGwb9p9vbwnXQIPlQrsF8Bozm8IyFGWxsfKT8dRljqmAEw
KLhaFgYdFrnliuYfmVMw+nSpdpTDVE0N4d7hd8mTN+WCvY0g6x9rv1uBPKK6lPgW
oZHskbzNLwiDXZ5vPKdoSCCIi3aQkCQd+6qxiQCVAgUQLm32FsDH/BbwDwQhAQFZ
qwP/cSSBsmwz45rZ8HP5NhUWxCUG1ZMmavp42mnhObIv03b680ufNMxp8nvbgAXU
WwCnHjmvdUZvzhLZs3g4xTyf6XXGddxVAzQZUEocreD92mzm9uJIi+uzMCcvu9Fm
4Pgu9Tux3ndjVahVBLZEoNoZVdPZAsa+PmkCEX0GFXK+0fmJAJUCBRAubfXabKHQ
hwZ57ZEBAYeaA/9aM5Oi5kaE9KjfVRwxSpyc2UWoEwXwNyabMVpp5HTqZjEnm/n+
0gsB/hcLUWDS1/vGeeP3UfHrDzctPBXwzRs+lAthLuHi8t99MHovELXy3crXEiIo

```
9jiUSXrYPca88OR+4dh4mt6FidgsxxZh9mFhMUL2IQwCFk8HpLVEC2Jfr4kAlQIF
EC5q5ajjEe6i7yfncQEBrd0D/1gxSJXMa4MtQbsYL0/QpEo4yYCs1dQ/M/IqHTy7
pfbPtVsVBmEyGL3Teu0F0RGC1e8odGEXQTVQazXbSrrbLXbG1v8uix3neCHfrAbi
uGOzgDd/JrY7mjqWSxRpvHsdeSlb0SW/++7u8izosXRUuw6Ykp2l6GacQvbxTJpt
kdSLtCR3aWV0c2UgdmVuZW1hIDx3aWV0c2VAcG9yY3VwaW5lLm9yZz6JARUDBRA1
O5tPy8QyP8SpYiUBAa6RB/4t7WU5FsXq9TaAslIoYtwsbWkPFZSlY1nZkMpoGOmw
dNzdc/MR5A8iC28E9LdZH+89VM1OnctR3MfKMqJoYBgFWmhxMo4VkDnBtMIZbMX+
QnMnp9piwM8T4VbQV49YMj5jbLCr2NUep8JIvd733OGs27SDjU25dHmkKvLf8A1U
BDGM9yKFL+OBJdLuzcTsddIUnLvysgiWAzB2MCriap1tgwYVgqB2DxztwayJusWY
iyv89Av8y8etDZFlAqfGdX/77E/iyQGVUi0kuHSNqePgAGe7idg4rLV3Zd05cNt6
CJ7s6LmOZI+iXA+8r890L+0VqRN4C/mNEQndtn9Bxv0tiQCVAwUQNNkG9NyA8qbV
Mny5AQGhEwP9GSNPhi0X+W0E35V4Iu/bvanFmjfwklkQbJaDhBMddhDtrJVzbZEv
e9AsQxEhK9me+Xql7ZQzOAjyM4c1aFO2+sq69H8z+e+pOkV/yWnRKIX9lVV4YJpK
ZLUSjKnV2Tvqo9EKXpFwjptO/YU1PZFEqXe/i3iIRecSOLJLqKvN3Zs=
=+cGX
-----END PGP PUBLIC KEY BLOCK-----
```

Appendix A Checksums

This appendix provides checksums for the individual files within the TCP Wrappers distribution.

```
MD5 (BLURB) = 627fc45308e852c446c3606647fa8c34
MD5 (Banners.Makefile) = e53315d5713278df908248602b129955
MD5 (CHANGES) = ff08c72b8c9c8d56ba9bf3e90d477639
MD5 (DISCLAIMER) = 071bd69cb78b18888ea5e3da5c3127fa
MD5 (Makefile) = 0037774577650534f898949d892144ec
MD5 (README) = 2452fb4f9d06500ec0634d7b64aaf76b
MD5 (README.IRIX) = 36603b049d5f89a26a300825c3021310
MD5 (README.NIS) = 147a07f2d3e673121dec4975849994e8
MD5 (clean_exit.c) = 1bac137fdc9c151351c0b33c9026421f
MD5 (diag.c) = 8f3d561785f3314a35a9de09d11ccdaa
MD5 (environ.c) = 9fa4c0f2fff89d00a4b1283730eab739
MD5 (eval.c) = b4fbd49308d5a8f77315167a4ee10339
MD5 (fakelog.c) = b329ab5443158e4c79f55710f9a675d0
MD5 (fix_options.c) = 99f3cb7841d8bf941bf6750fd7a96df1
MD5 (fromhost.c) = d880bab3c12c4109e95cdd69470e4ea3
```

```
MD5 (hosts_access.3) = 7993a6a2a27f729254bf29c13f48e9ab
MD5 (hosts_access.5) = 67085bc60fb9cbb70be7cb6490002923
MD5 (hosts_access.c) = cec0cba4a2df178e8857510704cc38f3
MD5 (hosts_ctl.c) = edad608818ee499ad0497dbabad43227
MD5 (hosts_options.5) = c4920a00f777844c6e8136e52e260264
MD5 (inetcf.c) = 02ccca613950bfe18706d0c39cbca9ea
MD5 (inetcf.h) = 2a7ac52919ccece4946943067455b1d8
MD5 (misc.c) = b74358d00ad758286a44c933fee4eda2
MD5 (miscd.c) = 720b62d42e8162cb7b696002e56ece6e
MD5 (mystdarg.h) = ce79d3c00d2ad46db810610c573bce2a
MD5 (myvsyslog.c) = 619fd9232e456e8ab75625f25dd58952
MD5 (ncr.c) = dc5262ae64eb1e3305bcfdc00e8fb9c9
MD5 (options.c) = 8b27d55628eb2b666b27f015ee2182b0
MD5 (patchlevel.h) = 92e06ff46922390163fdb46af95894f4
MD5 (percent_m.c) = 721472d1cc7cc8d4960d800057ed8ec1
MD5 (percent_x.c) = a406be699b48a19fb741fe8f31732698
MD5 (printf.ck) = 7dafed0315ad74bc7a28e7d747f29819
MD5 (ptx.c) = 9ab79f1b51877bbeeac82db794b25ad9
MD5 (refuse.c) = 5f2c0874378f640a86897f5531616dc7
MD5 (rfc931.c) = e629b1f5cfdc97dc43301ed1186f7c37
MD5 (safe_finger.c) = 7e4a788b375b7b05a60d24cd0c83b0b3
MD5 (scaffold.c) = ce9473ec933a5478d3522a15223c48c2
MD5 (scaffold.h) = 6b9d803d78ec0a6946f329d5a9856b53
MD5 (setenv.c) = 44209db39c4d3a173d2933b04f67320e
MD5 (shell_cmd.c) = 57b7371b951329db7b5f699e99798164
MD5 (socket.c) = 00f0890b1bc3e453ce44ccd64223b0c5
MD5 (strcasecmp.c) = 1e72db28013fc87fedcdbc155d8ba7fa
MD5 (tcpd.8) = eaee4abbff9c2853b4e5122ec1fb7a1b
MD5 (tcpd.c) = a8255a587f31a38b4a7485a5c8d904a3
MD5 (tcpd.h) = 076cf6456199450a4b81aec77165c716
MD5 (tcpdchk.8) = ed7b220f6ac7906ae326ac8fa3d04a11
MD5 (tcpdchk.c) = fe8a07ff2642e8b55922e6be510b9ed3
MD5 (tcpdmatch.8) = 85bc0335c865954ca534c9a17c666b53
MD5 (tcpdmatch.c) = 8af6daf4a1e9d9935956f1d31e54ab4f
MD5 (tli-sequent.c) = 6266612530ec81b4c3f90cbe34fcd108
MD5 (tli-sequent.h) = 9e8d21063e9157e7c2a4e9e3e3281e8b
MD5 (tli.c) = 7efc6e3c9915d6e8ca762342b540573d
MD5 (try-from.c) = c6a00f028c9578a881018b505857a05d
MD5 (update.c) = 77c218e0e6366d2327f52068f863d12b
MD5 (vfprintf.c) = 332dc8be89d5a59abc3036b490ba07d0
MD5 (workarounds.c) = d1e7b5abf95067313b7668d8c10a2c5c
```

The CERT Coordination Center wishes to thank Wietse Venema for his assistance in resolving this problem and Roy Arends of CERT-NL for valuable input in constructing this advisory. Additionally, we would like to thank Jochen Bauer of the Institute for Theoretical Physics at the University of Stuttgart for identifying an error in an earlier version of this advisory.

Wietse Venema expresses his appreciation to Andrew Brown of Crossbar Security, Inc. for noticing that the TCP Wrapper source code had been tampered with, and for informing the author of the incident.

Revision History

Fri January 22, 1999 Modified to reflect that the Trojan horse provides root access to intruders initiating connections from source port of 421 as opposed to a destination port of 421.

Added section indicating that the primary FTP archive for TCP Wrapper source has changed. Added an MD5 checksum and size for the correct version of the file tcp_wrappers_7.6.tar. Added MD5 checksums for individual files within the TCP Wrapper distribution.

2 CA-1999-02: Trojan Horses

Original issue date: February 5, 1999
Last revised: March 8, 1999
Minor typograhical corrections

A complete revision history is at the end of this file.

Systems Affected

Any system can be affected by Trojan horses.

Overview

Over the past few weeks, we have received an increase in the number of incident reports related to Trojan horses. This advisory includes descriptions of some of those incidents (Section II), some general information about Trojan horses (Sections I and V), and advice for system and network administrators, end users, software developers, and distributors (Section III).

Few software developers and distributors provide a strong means of authentication for software products. We encourage all software developers and distributors to do so. This means that until strong authentication of software is widely available, the problem of Trojan horses will persist. In the meantime, users and administrators are strongly encouraged to be aware of the risks as described in this document.

I. Description

A Trojan horse is an "apparently useful program containing hidden functions that can exploit the privileges of the user [running the program], with a resulting security threat. A Trojan horse does things that the program user did not intend" [Summers].

Trojan horses rely on users to install them, or they can be installed by intruders who have gained unauthorized access by other means. Then, an intruder attempting to subvert a system using a Trojan horse relies on other users running the Trojan horse to be successful.

II. Recent Incidents

Incidents involving Trojan horses include the following:

False Upgrade to Internet Explorer

Recent reports indicate wide distribution of an email message which claims to be a free upgrade to the Microsoft Internet Explorer web browser. However, we have confirmed with Microsoft that

they do not provide patches or upgrades via electronic mail, although they do distribute security bulletins by electronic mail.

The email message contains an attached executable program called *Ie0199.exe*. After installation, this program makes several modifications to the system and attempts to contact other remote systems. We have received conflicting information regarding the modifications made by the Trojan horse, which could be explained by the existence of multiple versions of the Trojan horse.

At least one version of the Trojan horse is accompanied by a message which reads, in part:

As an user of the Microsoft Internet Explorer, Microsoft Corporation provides you with this upgrade for your web browser. It will fix some bugs found in your Internet Explorer. To install the upgrade, please save the attached file (ie0199.exe) in some folder and run it.

The above message is not from Microsoft.

We encourage you to refer to the Microsoft Internet Explorer web site at the following location: http://www.microsoft.com/windows/ie/security/default.asp.

Please refer to the Section III below for general solutions to Trojan horses.

Trojan Horse Version of TCP Wrappers

We recently published "CA-99-01-Trojan-TCP-Wrappers" which said that some copies of the source code for the TCP Wrappers tool were modified by an intruder and contain a Trojan horse.

The advisory is available at the following location:
http://www.cert.org/advisories/CA-99-01-Trojan-TCP-Wrappers.html.

Trojan Horse Version of util-linux

The util-linux distribution includes several essential utilities for linux systems. We have confirmed with the authors of util-linux that a Trojan horse was placed in the file util-linux-2.9g.tar.gz on at least one ftp server between January 22, 1999, and January 24, 1999. This Trojan horse could have been distributed to mirror FTP sites.

Within the Trojan horse util-linux distribution the program */bin/login* was modified. The modifications included code to send email to an intruder that contains the host name and uid of users logging in. The code was also modified to provide anyone with access to a login prompt the capability of executing commands based on their input at the login prompt. There were no other functional modifications made to the Trojan horse util-linux distribution that we are aware of.

A quick check to ensure you do not have the Trojan horse installed is to execute the following command:

```
$ strings /bin/login | grep "HELO"
```

If that command returns the following output, then your machine has the Trojan horse version of util-linux-2.9g installed:

```
HELO 127.0.0.1
```

If the above command returns nothing, then you do not have this particular Trojan horse installed.

You cannot rely on the modification date of the file util-linux-2.9g.tar.gz because the Trojan horse version has the same size and time stamp as the original version.

In response to the distribution of this Trojan horse, the authors of util-linux have released util-linux-2.9h.tar.gz. This file is available via anonymous ftp from:
ftp://ftp.win.tue.nl/pub/linux/utils/util-linux/util-linux-2.9h.tar.gz.

Be sure to download and verify the PGP signature as well:
ftp://ftp.win.tue.nl/pub/linux/utils/util-linux/util-linux-2.9h.tar.gz.sign.

This package can be verified with the "Linux Kernel Archives" PGP Public Key, available from the following URL:http://www.kernel.org/signature.html.

Previous Trojan Horses

Trojan horses are not new entities. A classic description of a Trojan horse is given in [Thompson]. Additionally, you may wish to review the following documents for background and historical information about Trojan horses.

http://www.cert.org/advisories/CA-99-01-Trojan-TCP-Wrappers.html

http://www.cert.org/vul_notes/VN-98.07.backorifice.html

http://www.cert.org/advisories/CA-94.14.trojan.horse.in.IRC.client.for.UNIX.html

http://www.cert.org/advisories/CA-94.07.wuarchive.ftpd.trojan.horse.html

http://www.cert.org/advisories/CA-94.05.MD5.checksums.html

http://www.cert.org/advisories/CA-94.01.ongoing.network.monitoring.attacks.html

http://www.cert.org/advisories/CA-90.11.Security.Probes.html

III. Impact

Trojan horses can do anything that the user executing the program has the privileges to do. This includes

- deleting files that the user can delete
- transmitting to the intruder any files that the user can read
- changing any files the user can modify

- installing other programs with the privileges of the user, such as programs that provide unauthorized network access
- executing privilege-elevation attacks; that is, the Trojan horse can attempt to exploit a vulnerability to increase the level of access beyond that of the user running the Trojan horse. If this is successful, the Trojan horse can operate with the increased privileges.
- installing viruses
- installing other Trojan horses

If the user has administrative access to the operating system, the Trojan horse can do anything that an administrator can. The Unix 'root' account, the Microsoft Windows NT 'administrator' account, or any user on a single-user operating system has administrative access to the operating system. If you use one of these accounts, or a single-user operating system (e.g., Windows 95 or MacOS), keep in mind the potential for increased impact of a Trojan horse.

A compromise of any system on your network, including a compromise through Trojan horses, may have consequences for the other systems on your network. Particularly vulnerable are systems that transmit authentication material, such as passwords, over shared networks in cleartext or in a trivially encrypted form. This is very common. If a system on such a network is compromised via a Trojan horse (or another method), the intruder may be able to install a network sniffer and record usernames and passwords or other sensitive information as it traverses the network.

Additionally, a Trojan horse, depending on the actions it takes, may implicate your site as the source of an attack and may expose your organization to liability.

IV. How Trojan Horses Are Installed

Users can be tricked into installing Trojan horses by being enticed or frightened. For example, a Trojan horse might arrive in email described as a computer game. When the user receives the mail, they may be enticed by the description of the game to install it. Although it may in fact be a game, it may also be taking other action that is not readily apparent to the user, such as deleting files or mailing sensitive information to the attacker. As another example, an intruder may forge an advisory from a security organization, such as the CERT Coordination Center, that instructs system administrators to obtain and install a patch.

Other forms of "social engineering" can be used to trick users into installing or running Trojan horses. For example, an intruder might telephone a system administrator and pose as a legitimate user of the system who needs assistance of some kind. The system administrator might then be tricked into running a program of the intruder's design.

Software distribution sites can be compromised by intruders who replace legitimate versions of software with Trojan horse versions. If the distribution site is a central distribution site whose contents are mirrored by other distribution sites, the Trojan horse may be downloaded by many sites and spread quickly throughout the Internet community.

Because the Domain Name System (DNS) does not provide strong authentication, users may be tricked into connecting to sites different than the ones they intend to connect to. This could be exploited by an intruder to cause users to download a Trojan horse, or to cause users to expose confidential information.

Intruders may install Trojan horse versions of system utilities after they have compromised a system. Often, collections of Trojan horses are distributed in toolkits that an intruder can use to compromise a system and conceal their activity after the compromise, e.g., a toolkit might include a Trojan horse version of *ls* which does not list files owned by the intruder. Once an intruder has gained administrative access to your systems, it is very difficult to establish trust in it again without rebuilding the system from known-good software. For information on recovering after a compromise, please see http://www.cert.org/tech_tips/root_compromise.html.

A Trojan horse may be inserted into a program by a compiler that is itself a Trojan horse. For more information about such an attack, see [Thompson].

Finally, a Trojan horse may simply be placed on a web site to which the intruder entices victims. The Trojan horse may be in the form of a Java applet, JavaScript, ActiveX control, or other form of executable content.

V. Solutions

The best advice with respect to Trojan horses is to avoid them in the first place.

- System administrators (including the users of single-user systems) should take care to verify that every piece of software that is installed is from a trusted source and has not been modified in transit. When digital signatures are provided, users are encouraged to validate the signature (as well as validating the public key of the signer). When digital signatures are not available, you may wish to acquire software on tangible media such as CDs, which bear the manufacturer's logo. Of course, this is not foolproof either. Without a way to authenticate software, you may not be able to tell if a given piece of software is legitimate, regardless of the distribution media.
- We strongly encourage software developers and software distributors to use cryptographically strong validation for all software they produce or distribute. Any popular technique based on algorithms that are widely believed to be strong will provide users a strong tool to defeat Trojan horses.
- Anyone who invests trust in digital signatures must also take care to validate any public keys that may be associated with the signature. It is not enough for code merely to be signed -- it must be signed by a trusted source.
- Do not execute *anything* sent to you via unsolicited electronic mail.
- Use caution when executing content such as Java applets, JavaScript, or Active X controls from web pages. You may wish to configure your browser to disable the automatic execution of web page content.
- Apply the principle of least privilege in daily activity: do not retain or employ privileges that are not needed to accomplish a given task. For example, do not run with enhanced privilege, such as "root" or "administrator," ordinary tasks such as reading email.

- Install and configure a tool such as Tripwire® that will allow you to detect changes to system files in a cryptographically strong way. For more information about Tripwire®, see http://www.cert.org/ftp/tech_tips/security_tools,

  Note, however, that Tripwire® is not a foolproof guard against Trojan horses. For example, see http://www.cert.org/vul_notes/VN-98.02.kernel_mod.html.

- Educate your users regarding the danger of Trojan horses.

- Use firewalls and virus products that are aware of popular Trojan horses. Although it is impossible to detect all possible Trojan horses using a firewall or virus product (because a Trojan horse can be arbitrary code), they may aid you in preventing many popular Trojan horses from affecting your systems.

- Review the source code to any open source products you choose to install. Open source software has an advantage compared to proprietary software because the source code can be widely reviewed and any obvious Trojan horses will probably be discovered very quickly. However, open source software also tends to be developed by a wide variety of people with little or no central control. This makes it difficult to establish trust in a single entity. Keep in mind that reviewing source code may be impractical at best, and that some Trojan horses may not be evident from a review of the source as described in [Thompson].

- Adopt the use of cryptographically strong mutual authentication systems, such as *ssh*, for terminal emulation, X.509 public key certificates in web servers, *S/MIME* or *PGP* for electronic mail, and *kerberos* for a variety of services. Avoid the use of systems that trust the domain name system for authentication, such as *telnet*, ordinary http (as opposed to https), *ftp*, or *smtp*, unless your network is specifically designed to support that trust.

- Do not rely on timestamps, file sizes, or other file attributes when trying to determine if a file contains a Trojan horse.

- Exercise caution when downloading unauthenticated software. If you choose to install software that has not been signed by a trusted source, you may wish to wait for a period of time before installing it in order to see if a Trojan horse is discovered.

- We encourage all security organizations to digitally sign any advisories or other alerts. We also recommend that users validate any signatures, and beware of unsigned security advice. The CERT Coordination Center signs all ASCII copies of our advisories with our PGP key, available at: http://www.cert.org/pgp/CERT_PGP.key.

If you do fall victim to a Trojan horse, some anti-virus software may also be able to recognize, remove and repair the damage from the Trojan horse. However, if an intruder gains access to your systems via a Trojan horse, it may be difficult or impossible to establish trust in your systems. In this case, we recommend that you disconnect from the network and rebuild your systems from known-good software, being careful to apply all relevant patches and updates, to change all passwords, and to check other nearby systems. For information on how to rebuild a Unix system after a compromise, please see http://www.cert.org/tech_tips/root_compromise.html.

References

[Summers] Summers, Rita C. Secure Computing Threats and Safeguards, McGraw-Hill, 1997. An online reference is available from the publisher.

[Thompson] Thompson, Ken, "Reflections on Trusting Trust," Communications of the ACM 27(8) pp. 761-763 (Aug. 1984); Turing Award lecture.

Acknowledgment

Our thanks to Andries Brouwer for providing information regarding util-linux and to the many people who reported information about Trojan horse versions of Internet Explorer.

Revision History

```
Mar. 08, 1999  Minor typograhical corrections
```

3 CA-1999-03: FTP Buffer Overflows

Original issue date: February 11, 1999
Last revised: July 7, 1999
Updated information for Silicon Graphics, Inc. (SGI).

A complete revision history is at the end of this file.

Source: Netect, Inc.

To aid in the wide distribution of essential security information, the CERT Coordination Center is forwarding the following information from Netect, Inc. Netect, Inc. urges you to act on this information as soon as possible. See Appendix C for Netect, Inc. contact information. Please contact them if you have any questions or need further information.

==========FORWARDED TEXT STARTS HERE==========

```
Netect, Inc.

General Public Security Advisory

% Advisory: palmetto.ftpd

% Issue date: February 9, 1999

% Contact: Jordan Ritter <jpr5@netect.com>

% Revision: February 11, 1999

% Update: Appendices A and B corrected.

[Topic]

Remote buffer overflows in various FTP servers leads to potential
root compromise.

[Affected Systems]

Any server running the latest version of ProFTPD (1.2.0pre1) or the
latest version of Wuarchive ftpd (2.4.2-academ[BETA-18]).  wu-ftpd
is installed and enabled by default on most Linux variants such as
RedHat and Slackware Linux.  ProFTPD is new software recently
adopted by many major internet companies for its improved perfor-
mance and reliability.

Investigation of this vulnerability is ongoing; the below lists
software and operating systems for which Netect has definitive in-
formation. [Overview] Software that implements FTP is called an "ftp
```

server", "ftp daemon", or "ftpd". On most vulnerable systems, the ftpd software is enabled and installed by default.

There is a general class of vulnerability that exists in several popular ftp servers. Due to insufficient bounds checking, it is possible to subvert an ftp server by corrupting its internal stack space. By supplying carefully designed commands to the ftp server, intruders can force the the server to execute arbitrary commands with root privilege.

On most vulnerable systems, the ftpd software is installed and enabled by default.

[Impact]

Intruders who are able to exploit this vulnerability can ultimately gain interactive access to the remote ftp server with root privilege.

[Solution]

Currently there are several ways to exploit the ftp servers in question. One temporary workaround against an anonymous attack is to disable any world writable directories the user may have access to by making them read only. This will prevent an attacker from building an unusually large path, which is required in order to execute these particular attacks.

The permanent solution is to install a patch from your Vendor, or locate one provided by the Software's author or maintainer. See Appendices A and B for more specific information. Netect strongly encourages immediate upgrade and/or patching where available.

Netect provides a strong software solution for the automatic detection and removal of security vulnerabilities. Current HackerShield customers can protect themselves from this vulnerability by either visiting the Netect website and downloading the latest RapidFire(tm) update, or by enabling automatic RapidFire(tm) updates (no user intervention required).

Interested in protecting your network today? Visit the Netect website at http://www.netect.com/ and download a FREE 30 day copy of HackerShield, complete with all the latest RapidFire(tm) updates to safeguard your network from hackers.

[Appendix A, Software Information]

% ProFTPD

Current version: 1.2.0pre1, released October 19, 1998.

All versions prior to 1.2.0pre1: vulnerable.

Fix: will be incorporated into 1.2.0pre2.

Currently recommended action: upgrade to the new version when it becomes available, or apply the version 1.2.0pre1 patch found at: ftp://ftp.proftpd.org/patches/proftpd-1.2.0pre1-path_exploit2.patch

% wu-ftpd

Current version: 2.4.2 (beta 18), unknown release date.

All versions through 2.4.2 (beta 18): vulnerability dependant upon xctarget platform, probably vulnerable either due to OS-provided runtime vulnerability or through use of replacement code supplied with the source kit. No patches have been made available.

Fix: unknown.

Currently recommended action: Upgrade to wu-ftpd VR series.

% wu-ftpd VR series

Current version: 2.4.2 (beta 18) VR13, released January 28, 1999.

All versions prior to 2.4.2 (beta 18) VR10: vulnerable.

Fix: incorporated into VR10, released November 1, 1998.

Available from:ftp://ftp.vr.net/pub/wu-ftpd/

Filenames:

wu-ftpd-2.4.2-beta-18-vr13.tar.Z

wu-ftpd-2.4.2-beta-18-vr13.tar.gz

% BeroFTPD [NOT vulnerable]

Current version: 1.3.3, released February 7, 1999.

All versions prior to 1.2.0: vulnerable.

Fix: incorporated into 1.2.0, released October 26, 1998.

Available from: ftp://ftp.croftj.net/usr/bero/BeroFTPD/ and ftp://ftp.sunet.se/pub/nir/ftp/servers/BeroFTPD/

ftp://sunsite.cnlab-switch.ch/mirror/BeroFTPD/

Filename:

BeroFTPD-1.3.3.tar.gz

% NcFTPd [NOT vulnerable]

Current version: 2.4.0, released February 6, 1999.

All versions prior to 2.3.4: unknown.

Available from: http://www.ncftp.com/download/

Notes:

% NcFTPd 2.3.4 (libc5) ftp server has a remotely exploitable bug that results in the loss of the server's ability to log activity.

% This bug cannot be exploited to gain unintended or privileged access to a system running the NcFTPd 2.3.4 (libc5) ftp server, as tested

The bug was reproducible only on a libc5 Linux system. Linux glibc version of NcFTPd 2.3.4 ftp server is NOT vulnerable.

% The bug does not appear to be present in version NcFTPd 2.3.5 or later. Affected users may upgrade free of charge to the latest version.

Thanks go to Gregory Lundberg for providing the information regarding wu-ftpd and BeroFTPD.

[Appendix B, Vendors]

% RedHat Software, Inc.

% RedHat Version 5.2 and previous versions ARE vulnerable.

Updates will be available from: ftp://updates.redhat.com/5.2/<arch>

Filename: wu-ftpd-2.4.2b18-2.1.<arch>.rpm

% Walnut Creek CDROM and Patrick Volkerding

% Slackware All versions ARE vulnerable. Updates will be available from:

ftp://ftp.cdrom.com/pub/linux/slackware-3.6/slakware/n8/

ftp://ftp.cdrom.com/pub/linux/slackware-current/slakware/n8/

Filenames

tcpip1.tgz (3.6) [971a5f57bec8894364c1e0d358ffbfd4]

tcpip1.tgz (current) [e1e9a9a50ad65bab1e120a7bf60f6011]

Notes:

% The md5 checksums are current for the above mentioned Revision date only.

% Caldera Systems, Inc.

% OpenLinux Latest version IS vulnerable. Updates will be available from: ftp://ftp.calderasystems.com/pub/OpenLinux/updates/

% SCO

% UnixWare Version 7.0.1 and earlier (except 2.1.x) IS vulnerable.

% OpenServer Versions 5.0.5 and earlier IS vulnerable.

% CMW+ Version 3.0 is NOT vulnerable.

% Open Desktop/Server Version 3.0 is NOT vulnerable.

Binary versions of ftpd will be available shortly from the SCO ftp

site:

ftp://ftp.sco.com/SSE/sse021.ltr - cover letter

ftp://ftp.sco.com/SSE/sse021.tar.Z - replacement binaries

Notes:

This fix is a binary for the following SCO operating systems:

% SCO UnixWare 7.0.1 and earlier releases (not UnixWare 2.1.x)

% SCO OpenServer 5.0.5 and earlier releases

For the latest security bulletins and patches for SCO products, please refer to http://www.sco.com/security/.

% IBM Corporation

% AIX Versions 4.1.x, 4.2.x, and 4.3.x ARE NOT vulnerable.

% Hewlett-Packard

% HPUX Versions 10.x and 11.x ARE NOT vulnerable. HP is continuing their investigation.

% Sun Microsystems, Inc.

% SunOS All versions ARE NOT vulnerable.

% Solaris All versions ARE NOT vulnerable.

% Microsoft, Inc.

% IIS Versions 3.0 and 4.0 ARE NOT vulnerable.

% Compaq Computer Corporation

% Digital UNIX V40b - V40e ARE NOT vulnerable.

% TCP/IP(UCX) for OpenVMS V4.1, V4.2, V5.0 ARE NOT vulnerable.

% Silicon Graphics, Inc. (SGI)

% IRIX and Unicos

Currently, Silicon Graphics, Inc. is investigating and no further information is available for public release at this time. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution method including the wiretap mailing list. Silicon Graphics Security Headquarters http://www.sgi.com/Support/security/

% NetBSD

% NetBSD All versions ARE NOT vulnerable.

[Appendix C, Netect Contact Information]

The contact for this advisory is Jordan Ritter <jpr5@netect.com>. PGP signed/encrypted email is preferred.

Visit http://www.netect.com/ for more information.

==========FORWARDED TEXT ENDS HERE==========

CERT/CC has received the following additional information:

Fujitsu [NOT vulnerable]

Fujitsu's UXP/V operating system is not vulnerable. The reason behind this is the ftod of UXP/V does not have static buffers to store the current working directory.

Silicon Graphics, Inc. (SGI)

IRIX and Unicos

IRIX operating system is not vulnerable.

Cray Unicos and Unicos MK

Unicos and Unicos/MK is not vulnerable.

Revision History

Jul 07, 1999 Added updated information for Silicon Graphics, Inc. (SGI)

Mar 16, 1999 Additional information for Fujitsu has been added.

4 CA-1999-04: Melissa Macro Virus

Original issue date: March 27, 1999
Last revised: March 31, 1999

A complete revision history is at the end of this file.

Systems Affected

- Machines with Microsoft Word 97 or Word 2000
- Any mail handling system could experience performance problems or a denial of service as a result of the propagation of this macro virus.

Overview

At approximately 2:00 PM GMT-5 on Friday March 26 1999 we began receiving reports of a Microsoft Word 97 and Word 2000 macro virus which is propagating via email attachments. The number and variety of reports we have received indicate that this is a widespread attack affecting a variety of sites.

Our analysis of this macro virus indicates that human action (in the form of a user opening an infected Word document) is required for this virus to propagate. It is possible that under some mailer configurations, a user might automatically open an infected document received in the form of an email attachment. This macro virus is not known to exploit any new vulnerabilities. While the primary transport mechanism of this virus is via email, any way of transferring files can also propagate the virus.

Anti-virus software vendors have called this macro virus the Melissa macro or W97M_Melissa virus.

In addition to this advisory, please see the Melissa Virus FAQ (Frequently Asked Questions) document available at: http://www.cert.org/tech_tips/Melissa_FAQ.html.

I. Description

The Melissa macro virus propagates in the form of an email message containing an infected Word document as an attachment. The transport message has most frequently been reported to contain the following Subject header

```
Subject: Important Message From <name>
```

Where <name> is the full name of the user sending the message.

The body of the message is a multipart MIME message containing two sections. The first section of the message (Content-Type: text/plain) contains the following text.

Here is that document you asked for ... don't show anyone else ;-)

The next section (Content-Type: application/msword) was initially reported to be a document called "list.doc". This document contains references to pornographic web sites. As this macro virus spreads we are likely to see documents with other names. In fact, under certain conditions the virus may generate attachments with documents created by the victim.

When a user opens an infected .doc file with Microsoft Word97 or Word2000, the macro virus is immediately executed if macros are enabled.

Upon execution, the virus first lowers the macro security settings to permit all macros to run when documents are opened in the future. Therefore, the user will not be notified when the virus is executed in the future.

The macro then checks to see if the registry key

"HKEY_Current_User\Software\Microsoft\Office\Melissa?"

has a value of **"... by Kwyjibo"**. If that registry key does not exist or does not have a value of **"... by Kwyjibo"**, the virus proceeds to propagate itself by sending an email message in the format described above to the first 50 entries in every Microsoft Outlook MAPI address book readable by the user executing the macro. Keep in mind that if any of these email addresses are mailing lists, the message will be delivered to everyone on the mailing lists. In order to successfully propagate, the affected machine must have Microsoft Outlook installed; however, Outlook does not need to be the mailer used to read the message.

This virus can not send mail on systems running MacOS; however, the virus can be stored on MacOS.

Next, the macro virus sets the value of the registry key to **"... by Kwyjibo"**. Setting this registry key causes the virus to only propagate once per session. If the registry key does not persist through sessions, the virus will propagate as described above once per every session when a user opens an infected document. If the registry key persists through sessions, the virus will no longer attempt to propagate even if the affected user opens an infected document.

The macro then infects the Normal.dot template file. By default, all Word documents utilize the Normal.dot template; thus, any newly created Word document will be infected. Because unpatched versions of Word97 may trust macros in templates the virus may execute without warning. For more information please see: http://www.microsoft.com/security/bulletins/ms99-002.asp.

Finally, if the minute of the hour matches the day of the month at this point, the macro inserts into the current document the message "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

Note that if you open an infected document with macros disabled and look at the list of macros in this document, neither Word97 nor Word2000 list the macro. The code is actually VBA (Visual Basic for Applications) code associated with the "document.open" method. You can see the code by going into the Visual Basic editor.

If you receive one of these messages, keep in mind that the message came from someone who is affected by this virus and they are not necessarily targeting you. We encourage you to contact any users from which you have received such a message. Also, we are interested in understanding the scope of this activity; therefore, we would appreciate if you would report any instance of this activity to us according to our Incident Reporting Guidelines document available at: http://www.cert.org/tech_tips/incident_reporting.html.

II. Impact

- Users who open an infected document in Word97 or Word2000 with macros enabled will infect the Normal.dot template causing any documents referencing this template to be infected with this macro virus. If the infected document is opened by another user, the document, including the macro virus, will propagate. Note that this could cause the user's document to be propagated instead of the original document, and thereby leak sensitive information.
- Indirectly, this virus could cause a denial of service on mail servers. Many large sites have reported performance problems with their mail servers as a result of the propagation of this virus.

III. Solutions

Block messages with the signature of this virus at your mail transfer agents or other central point of control.

With Sendmail

Nick Christenson of sendmail.com provided information about configuring sendmail to filter out messages that may contain the Melissa virus. This information is available from the follow URL: http://www.sendmail.com/blockmelissa.html.

With John Hardin's Procmail security filter package

More information is available from:
ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html.

With Innosoft's PMDF

More information is available from:
http://www.innosoft.com/iii/pmdf/virus-word-emergency.html.

Utilize virus scanners

Most virus scanning tools will detect and clean macro viruses. In order to detect and clean current viruses you must keep your scanning tools up to date with the latest definition files.

Computer Associates

Virus signature versions that detect and cure melissa virus.

Windows NT 3.x & 4.x	4.19d
Windows 95	4.19e
Windows 98	4.19e
Windows 3.1	4.19e
Netware 3.x, 4.x & 5.0	4.19e

Any of the above virus signatures files can be downloaded at: http://www.support.cai.com.

McAfee / Network Associates

http://vil.mcafee.com/vil/vm10118.asp

http://www.avertlabs.com/public/datafiles/valerts/vinfo/melissa.asp

Sophos

http://www.sophos.com/downloads/ide/index.html#melissa

Symantec

http://www.symantec.com/avcenter/venc/data/mailissa.html

Trend Micro

http://housecall.antivirus.com/smex_housecall/technotes.html

Encourage users at your site to disable macros in Microsoft Word

Notify all of your users of the problem and encourage them to disable macros in Word. You may also wish to encourage users to disable macros in any product that contains a macro language as this sort of problem is not limited to Microsoft Word.

In Word97 you can disable automatic macro execution (click Tools/Options/General then turn on the 'Macro virus protection' checkbox). In Word2000 macro execution is controlled by a security

level variable similar to Internet Explorer (click on Tools/Macro/Security and choose High, Medium, or Low). In that case, 'High' silently ignores the VBA code, Medium prompts in the way Word97 does to let you enable or disable the VBA code, and 'Low' just runs it.

Word2000 supports Authenticode on the VB code. In the 'High' setting you can specify sites that you trust and code from those sites will run.

General protection from Word Macro Viruses

For information about macro viruses in general, we encourage you to review the document "Free Macro AntiVirus Techniques" by Chengi Jimmy Kuo which is available at: http://www.nai.com/services/support/vr/free.asp.

Additional Information

- For more information about the Melissa virus please see the Melissa Virus FAQ (Frequently Asked Questions) document available at: http://www.cert.org/tech_tips/Melissa_FAQ.html.

- We have received a number of reports from people confusing the Happy99.exe Trojan Horse with the Melissa virus. For more information about Happy99.exe please see: http://www.cert.org/incident_notes/IN-99-02.html.

- The Department of Energy's Computer Incident Advisory Capability (CIAC) has published several documents that you may wish to examine. These are available at available at http://www.ciac.org/ciac/bulletins/j-037.shtml and http://ciac.llnl.gov/ciac/bulletins/i-023.shtml.

- Microsoft Corporation has published information about this macro virus. Their document is available from: http://officeupdate.microsoft.com/articles/macroalert.htm.

Acknowledgements

We would like to thank Jimmy Kuo of Network Associates, Eric Allman and Nick Christenson of sendmail.com, Dan Schrader of Trend Micro, Jason Garms and Karan Khanna of Microsoft, Ned Freed of Innosoft, and John Hardin for providing information used in this advisory.

Additionally we would like to thank the many sites who reported this activity.

Revision History

```
March 28, 1999:  Changed the reference to the sendmail patches from
ftp.cert.org to www.sendmail.com. Added information for Innosoft,
Sophos, and John Hardin's procmail filter kit.
```

March 29, 1999: Formatting changes

March 29, 1999: Added information for Computer Associates

March 29, 1999: Fixed a broken link

March 29, 1999: Added a link to information at Microsoft, added a link to information about Happy99.exe, added information about MacOS, and clairfied that only MS Outlook MAPI address books are involved.

March 31, 1999: Added links to the Melissa FAQ

5 CA-1999-05: Vulnerability in statd exposes vulnerability in automountd

Original issue date: June 9, 1999
Last revised: November 9, 1999
Added Vendor information for IBM Corporation.
Source: CERT/CC

Systems Affected

Systems running older versions of rpc.statd and automountd

I. Description

This advisory describes two vulnerabilities that are being used together by intruders to gain access to vulnerable systems. The first vulnerability is in rpc.statd, a program used to communicate state changes among NFS clients and servers. The second vulnerability is in automountd, a program used to automatically mount certain types of file systems. Both of these vulnerabilities have been widely discussed on public forums, such as **BugTraq**, and some vendors have issued security advisories related to the problems discussed here. Because of the number of incident reports we have received, however, we are releasing this advisory to call attention to these problems so that system and network administrators who have not addressed these problems do so immediately. For more information about attacks using various RPC services please see CERT® Incident Note IN-99-04 http://www.cert.org/incident_notes/IN-99-04.html

The vulnerability in rpc.statd allows an intruder to call arbitrary rpc services with the privileges of the rpc.statd process. The called rpc service may be a local service on the same machine or it may be a network service on another machine. Although the form of the call is constrained by rpc.statd, if the call is acceptable to another rpc service, the other rpc service will act on the call as if it were an authentic call from the rpc.statd process.

The vulnerability in automountd allows a local intruder to execute arbitrary commands with the privileges of the automountd process. This vulnerability has been widely known for a significant period of time, and patches have been available from vendors, but many systems remain vulnerable because their administrators have not yet applied the appropriate patches.

By exploiting these two vulnerabilities simultaneously, a remote intruder is able to "bounce" rpc calls from the rpc.statd service to the automountd service on the same targeted machine. Although on many systems the automountd service does not normally accept traffic from the network, this combination of vulnerabilities allows a remote intruder to execute arbitrary commands with the administrative privileges of the automountd service, typically root.

Note that the rpc.statd vulnerability described in this advisory is distinct from the vulnerabilities described in CERT Advisories CA-96.09 and CA-97.26.

II. Impact

The vulnerability in rpc.statd may allow a remote intruder to call arbitrary rpc services with the privileges of the rpc.statd process, typically root. The vulnerablility in automountd may allow a local intruder to execute arbitrary commands with the privileges of the automountd service.

By combining attacks exploiting these two vulnerabilities, a remote intruder is able to execute arbitrary commands with the privileges of the automountd service.

Note

It may still be possible to cause rpc.statd to call other rpc services even after applying patches which reduce the privileges of rpc.statd. If there are additional vulnerabilities in other rpc services (including services you have written), an intruder may be able to exploit those vulnerabilities through rpc.statd. At the present time, we are unaware of any such vulnerabilitity that may be exploited through this mechanism.

III. Solutions

Install a patch from your vendor

Appendix A contains input from vendors who have provided information for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Caldera

Caldera's currently not shipping statd.

Compaq Computer Corporation

SOURCE: Compaq Computer Corporation
Compaq Services
Software Security Response Team USA

This reported problem has not been found to affect the as shipped, Compaq's Tru64/UNIX Operating Systems Software.
- Compaq Computer Corporation

Data General

We are investigating. We will provide an update when our investigation is complete.

Hewlett-Packard Company

HP is vulnerable to a remote attack against automountd.

Please see the following document for details on workarounds:

HPSBUX9910-104 Security Advisory regarding automountd

Patch development is in progress.

IBM Corporation

AIX is not vulnerable.

IBM and AIX are registered trademarks of International Business Machines Corporation.

The Santa Cruz Operation, Inc.

No SCO products are vulnerable.

Silicon Graphics, Inc.

% IRIX

% rpc.statd
IRIX 6.2 and above ARE NOT vulnerable.
IRIX 5.3 is vulnerable, but no longer supported.

% automountd
With patches from SGI Security Advisory 19981005-01-PX installed,
IRIX 6.2 and above ARE NOT vulnerable.

% Unicos

Currently, SGI is investigating and no further information is
available for public release at this time.

As further information becomes available, additional advisories
will be issued via the normal SGI security information distribution
method including the wiretap mailing list.

SGI Security Headquarters
http://www.sgi.com/Support/security

Sun Microsystems Inc.

The following patches are available:

rpc.statd:

Patch OS Version
_____

106592-02 SunOS 5.6
106593-02 SunOS 5.6_x86
104166-04 SunOS 5.5.1
104167-04 SunOS 5.5.1_x86
103468-04 SunOS 5.5
103469-05 SunOS 5.5_x86
102769-07 SunOS 5.4
102770-07 SunOS 5.4_x86
102932-05 SunOS 5.3

The fix for this vulnerability was integrated in SunOS 5.7 (Solaris 7) before it was released.

automountd:
104654-05 SunOS 5.5.1
104655-05 SunOS 5.5.1_x86
103187-43 SunOS 5.5
103188-43 SunOS 5.5_x86
101945-61 SunOS 5.4
101946-54 SunOS 5.4_x86
101318-92 SunOS 5.3

SunOS 5.6 (Solaris 2.6) and SunOS 5.7 (Solaris 7) are not vulnerable.

Sun security patches are available at:
http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pub-patches

Our thanks to Olaf Kirch of Caldera for his assistance in helping us understand the problem and Chok Poh of Sun Microsystems for his assistance in helping us construct this advisory.

Revision History

October 22, 1999 Updated vendor information for Hewlett-Packard Company

July 22, 1999 Added link to IN-99-04 in the "Description" section.

November 9, 1999 Added vendor information for IBM Corporation.

6 CA-1999-06: ExploreZip Trojan Horse Program

Original issue date: Thursday June 10, 1999
Last revised: June 14, 1999
Added information about the program's self-propagation via networked shares; also updated anti-virus vendor URLs.
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Machines running Windows 95, Windows 98, or Windows NT.
- Machines with filesystems and/or shares that are writable by a user of an infected system.
- Any mail handling system could experience performance problems or a denial of service as a result of the propagation of this Trojan horse program.

Overview

The CERT Coordination Center continues to receive reports and inquiries regarding various forms of malicious executable files that are propagated as file attachments in electronic mail.

During the second week of June 1999, the CERT/CC began receiving reports of sites affected by ExploreZip, a Trojan horse/worm program that affects Windows systems and has propagated in email attachments. The number and variety of reports we have received indicate that this has the potential to be a widespread attack affecting a variety of sites.

I. Description

Our original analysis indicated that the ExploreZip program is a Trojan horse, since it initially requires a victim to open or run an email attachment in order for the program to install a copy of itself and enable further propagation. Further analysis has shown that, once installed, the program may also behave as a worm, and it may be able to propagate itself, without any human interaction, to other networked machines that have certain writable shares.

The ExploreZip Trojan horse has been propagated between users in the form of email messages containing an attached file named *zipped_files.exe*. Some email programs may display this attachment with a "WinZip" icon. The body of the email message usually appears to come from a known email correspondent, and typically contains the following text:

> *I received your email and I shall send you a reply ASAP.*
> *Till then, take a look at the attached zipped docs.*

The subject line of the message may not be predictable and may appear to be sent in reply to previous email.

Opening the *zipped_files.exe* file causes the program to execute. It is possible under some mailer configurations that a user might automatically open a malicious file received in the form of an email attachment. When the program is run, an error message is displayed:

> *Cannot open file: it does not appear to be a valid archive. If this file is part of a ZIP format backup set, insert the last disk of the backup set and try again. Please press F1 for help.*

Destruction of files

- The program searches local and networked drives (drive letters C through Z) for specific file types and attempts to erase the contents of the files, leaving a zero byte file. The targets may include Microsoft Office files, such as .doc, .xls, and .ppt, and various source code files, such as .c, .cpp, .h, and .asm.
- The program may also be able to delete files that are writable to it via SMB/CIFS file sharing. The program appears to look through the network neighborhood and delete any files that are shared and writable, even if those shares are not mapped to networked drives on the infected computer.
- The program appears to continually delete the contents of targeted files on any mapped networked drives.

The program does not appear to delete files with the "hidden" or "system" attribute, regardless of their extension.

System modifications

- The *zipped_files.exe* program creates a copy of itself in a file called *explore.exe* in the following location(s):

  On Windows 98 - C:\WINDOWS\SYSTEM\Explore.exe
  On Windows NT - C:\WINNT\System32\Explore.exe

This *explore.exe* file is an identical copy of the *zipped_files.exe* Trojan horse, and the file size is 210432 bytes.
MD5 (Explore.exe) = 0e10993050e5ed199e90f7372259e44b

- On Windows 98 systems, the *zipped_files.exe* program creates an entry in the *WIN.INI* file:

run=C:\WINDOWS\SYSTEM\Explore.exe

On Windows NT systems, an entry is made in the system registry:

[HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows]
run = "C:\WINNT\System32\Explore.exe"

Propagation via file sharing

Once *explore.exe* is running, it takes the following steps to propagate to other systems via file sharing:

- Each time the program is executed, the program will search the network for all shares that contain a *WIN.INI* file with a valid "[windows]" section in the file.
- For each such share that it finds, the program will attempt to
- copy itself to a file named *_setup.exe* on that share
- modify the *WIN.INI* file on that share by adding the entry "run=_setup.exe"

The account running the program on the original infected machine needs to have permission to write to the second victim's shared directory. (That is, no vulnerabilities are being exploited in order for the program to spread in this manner.)

The *_setup.exe* file is identical to the *zipped_files.exe* and *explore.exe* files on the original infected machine.

- The original infected system will continue to scan shares that have been mapped to a local drive letter containing a valid WIN.INI file. For each such share that is found, the program will "re-infect" the victim system as described above.

On Windows 98 systems that have a "run=_setup.exe" entry in the *WIN.INI* file (as described previously), the *C:\WINDOWS_setup.exe* program is executed automatically whenever a user logs in. On Windows NT systems, a "run=_setup.exe" entry in the *WIN.INI* file does not appear to cause the program to be executed automatically.

When run as *_setup.exe*, the program will attempt to

- make another copy of itself in C:\WINDOWS\SYSTEM\Explore.exe
- modify the *WIN.INI* file again by replacing the "run=_setup.exe" entry with "run=C:\WINDOWS\SYSTEM\Explore.exe"

Note that when the program is run as _setup.exe, it configures the system to later run as explore.exe. But when run as explore.exe, it attempts to infect shares with valid WIN.INI files by configuring those files to run _setup.exe. Since this infection process includes local shares, affected systems may exhibit a "ping pong" behavior in which the infected host alternates between the two states.

Propagation via email

The program propagates by replying to any new email that is received by the infected computer. The reply messages are similar to the original email described above, each containing another copy of the *zipped_files.exe* attachment.

We will continue to update this advisory with more specific information as we are able to confirm details. Please check the CERT/CC web site for the current version containing a complete revision history.

II. Impact

- Users who execute the *zipped_files.exe* Trojan horse will infect the host system, potentially causing targeted files to be destroyed.
- Users who execute the Trojan horse may also infect other networked systems that have writable shares.
- Because of the large amount of network traffic generated by infected machines, network performance may suffer.
- Indirectly, this Trojan horse could cause a denial of service on mail servers. Several large sites have reported performance problems with their mail servers as a result of the propagation of this Trojan horse.

III. Solution

Use virus scanners

While many anti-virus products are able to detect and remove the executables locally, because of the continuous re-infection process, simply removing all copies of the program from an infected system may leave your system open to re-infection at a later time, perhaps immediately. To prevent re-infection, you must not serve any shares containing a WIN.INI file to any potentially infected machines. If you share files with everyone in your domain, then you must disable shares with WIN.INI files until every machine on your network has been disinfected.

In order to detect and clean current viruses, you must keep your scanning tools up to date with the latest definition files. Please see the following anti-virus vendor resources for more information about the characteristics and removal techniques for the malicious file known as ExploreZip.

Aladdin Knowledge Systems, Inc.
http://www.esafe.com/vcenter/explore.html

Central Command
http://www.avp.com/zippedfiles/zippedfiles.html

Command Software Systems, Inc
http://www.commandcom.com/html/virus/explorezip.html

Computer Associates
http://www.cai.com/virusinfo/virusalert.htm

Data Fellows
http://www.datafellows.com/news/pr/eng/19990610.htm

McAfee, Inc. (a Network Associates company)
http://www.mcafee.com/viruses/explorezip/default.asp

Network Associates Incorporated
http://www.avertlabs.com/public/datafiles/valerts/vinfo/va10185.asp

Sophos, Incorporated
http://www.sophos.com/downloads/ide/index.html#explorez

Symantec
http://www.symantec.com/avcenter/venc/data/worm.explore.zip.html

Trend Micro Incorporated
http://www.antivirus.com/vinfo/alerts.htm

Additional sources of virus information are listed at
http://www.cert.org/other_sources/viruses.html.

Additional suggestions

- Blocking Netbios traffic at your network border may help prevent propagation via shares from outside your network perimeter.
- Disable file serving on workstations. You will not be able to share your files with other computers, but you will be able to browse and get files from servers. This will prevent your workstation from being infected via file sharing propagation.
- Maintain a regular, off-line, backup cycle.

General protection from email Trojan horses and viruses

Some previous examples of malicious files known to have propagated through electronic mail include

- False upgrade to Internet Explorer - discussed in CA-99-02
  http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html
- Melissa macro virus - discussed in CA-99-04
  http://www.cert.org/advisories/CA-99-04-Melissa-Macro-Virus.html
- Happy99.exe Trojan Horse - discussed in IN-99-02
  http://www.cert.org/incident_notes/IN-99-02.html
- CIH/Chernobyl virus - discussed in IN-99-03
  http://www.cert.org/incident_notes/IN-99-03.html

In each of the above cases, the effects of the malicious file are activated only when the file in question is executed. Social engineering is typically employed to trick a recipient into executing the malicious file. Some of the social engineering techniques we have seen used include

- Making false claims that a file attachment contains a software patch or update

- Implying or using entertaining content to entice a user into executing a malicious file
- Using email delivery techniques which cause the message to appear to have come from a familiar or trusted source
- Packaging malicious files in deceptively familiar ways (e.g., use of familiar but deceptive program icons or file names)

The best advice with regard to malicious files is to avoid executing them in the first place. CERT advisory CA-99-02 discusses Trojan horses and offers suggestions to avoid them (please see Section V).

http://www.cert.org/advisories/CA-99-02-Trojan-Horses.html

Revision History

```
June 10, 1999:  Initial release

June 11, 1999:  Added information about the appearance of the at-
tached file

Added information from Aladdin Knowledge Systems, Inc.

June 14, 1999:  Added information about the program's self-propaga-
tion via networked shares; also updated anti-virus vendor URLs
```

7 CA-1999-07: IIS Buffer Overflow

Original release date: June 16, 1999
Last revised: June 18, 1999
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Machines running Microsoft Internet Information Server 4.0

I. Description

Buffer overflow vulnerabilities affecting Microsoft Internet Information Server 4.0 have been discovered in several libraries, including libraries that handle .HTR, .STM, and .IDC files.

A tool to exploit at least one of the vulnerabilities has been publicly released.

II. Impact

These vulnerabilities allow remote intruders to execute arbitrary code with the privileges of the IIS server. Additionally, intruders can use this vulnerability to crash vulnerable IIS processes.

III. Solution

Microsoft has released and updated Microsoft Security Bulletin MS99-019, which points to a patch for these vulnerabilities. We encourage you to read this bulletin, available from http://www.microsoft.com/security/bulletins/ms99-019.asp.

We will update this advisory as more information becomes available. Please check the CERT/CC Web site for the most current revision.

Our thanks to Jason Garms and Scott Culp of Microsoft for providing information contained in this advisory.

Revision History

```
June 16, 1999:  Initial release

June 18, 1999:  Added information about .STM and .IDC files.
```

8 CA-1999-08: Buffer Overflow Vulnerability in Calendar Manager Service Daemon, rpc.cmsd

Original release date: July 16, 1999
Last revised: January 7, 2000
Updated HP vendor information.
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running the Calendar Manager Service daemon, often named rpc.cmsd

I. Description

A buffer overflow vulnerability has been discovered in the Calendar Manager Service daemon, rpc.cmsd. The rpc.cmsd daemon is frequently distributed with the Common Desktop Environment (CDE) and Open Windows.

II. Impact

Remote and local users can execute arbitrary code with the privileges of the rpc.cmsd daemon, typically root. Under some configurations rpc.cmsd runs with an effective userid of daemon, while retaining root privileges.

This vulnerability is being exploited in a significant number of incidents reported to the CERT/CC. An exploit script was posted to BUGTRAQ. For more information about attacks using various RPC services please see CERT® Incident Note IN-99-04 http://www.cert.org/incident_notes/IN-99-04.html

III. Solution

Install a patch from your vendor

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

We will update this advisory as more information becomes available. Please check the CERT/CC Web site for the most current revision.

Disable the rpc.cmsd daemon

If you are unable to apply patches to correct this vulnerability, you may wish to disable the rpc.cmsd daemon. If you disable rpc.cmsd, it may affect your ability to manage calendars.

Appendix A Vendor Information

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable.

Hewlett-Packard Company

Patches are available. Please see the following document for details:

HPSBUX9908-102 Security Vulnerability in rpc.cmsd

IBM Corporation

AIX is not vulnerable to the rpc.cmsd remote buffer overflow.
IBM and AIX are registered trademarks of International Business Machines Corporation.

Santa Cruz Operation, Inc.

SCO is investigating this problem. The following SCO product contains CDE and is potentially vulnerable:

SCO UnixWare 7

The following SCO products do not contain CDE, and are therefore believed not to be vulnerable:

- SCO UnixWare 2.1
- SCO OpenServer 5
- SCO Open Server 3.0
- SCO CMW+

SCO will provide further information and patches if necessary as soon as possible at http://www.sco.com/security.

Silicon Graphics, Inc.

IRIX does not have dtcm or rpc.cmsd and therefore is NOT vulnerable.

UNICOS does not have dtcm or rpc.cmsd and therefore is NOT vulnerable.

Sun Microsystems, Inc.

The following patches are available:

OpenWindows:

```
SunOS version     Patch ID
```

SunOS 5.5.1	104976-04
SunOS 5.5.1_x86	105124-03
SunOS 5.5	103251-09
SunOS 5.5_x86	103273-07
SunOS 5.3	101513-14
SunOS 4.1.4	100523-25
SunOS 4.1.3_U1	100523-25

CDE:

CDE version	Patch ID
1.3	107022-03
1.3_x86	107023-03
1.2	105566-07
1.2_x86	105567-08

Patches for SunOS 5.4 and CDE 1.0.2 and 1.0.1 will be available within a week of the release of this advisory.

Sun security patches are available at: http://sunsolve.sun.com/pub-cgi/show.pl?target=patches/patch-license&nav=pubpatches.

The CERT Coordination Center would like to thank Chok Poh of Sun Microsystems, David Brumley of Stanford University, and Elias Levy of Security Focus for their assistance in preparing this advisory.

Revision History

January 7, 2000 Updated HP vendor information

July 22, 1999 Added link to IN-99-04 in the "Impact" section

July 20, 1999 Updated the advisory title

July 16, 1999 Initial release

9 CA-1999-09: Array Services deFA-19ult configuration

Original release date: July 19, 1999
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- IRIX systems running the Array Services daemon
- UNICOS systems running the Array Services daemon

I. Description

A vulnerability has been discovered in the default configuration of the Array Services daemon, arrayd. Array Services are used to manage a cluster of systems. The default configuration file, arrayd.auth, disables authentication and does not provide adequate protection for systems connected to an untrusted network.

SGI has published the following document describing the vulnerability and solutions: ftp://sgigate.sgi.com/security/19990701-01-P.

II. Impact

On systems installed with the default configuration, remote and local users can execute arbitrary commands as root.

III. Solution

Use "SIMPLE" authentication

Reconfigure arrayd to use "SIMPLE" authentication. For more information about reconfiguring arrayd, please see the SGI security bulletin.

Disable the arrayd daemon

If you do not need the capabilities provided by the arrayd daemon, you may wish to disable the daemon.

The CERT Coordination Center would like to thank Yuri Volobuev and the SGI Security Team for their assistance in preparing this advisory.

Revision History

```
July 19, 1999:  Initial release
```

10 CA-1999-10: Insecure Default Configuration on RaQ2 Servers

Original issue date: July 30, 1999
Last revised: July 25, 2001
Source: CERT/CC
See also: Cobalt Networks Security Announcement

A complete revision history is at the end of this file.

Systems Affected

- Cobalt Networks RaQ2 single rack unit Internet servers

I. Description

A vulnerability has been discovered in the default configuration of Cobalt Networks RaQ2 servers that allows remote users to install arbitrary software packages to the system. RaQ2 servers are configured with an administrative webserver to process remote requests to manage the unit. Systems installed with the default configuration have insufficient access control mechanisms to prevent remote users from adding arbitrary software packages to the system using this webserver.

A document published by Cobalt Networks describes the vulnerability and solutions in more detail: http://noram.cobaltnet.com/support/security/index.html.

II. Impact

Any remote user who can establish a connection to an administrative port on a vulnerable RaQ2 server can install arbitrary software packages on the server. This access can then be used to gain root privileges on the system.

III. Solution

Configure your Systems to Guard Against this Vulnerability

Install the patches provided by Cobalt Networks:

> http://www.cobaltnet.com/patches/RaQ2-Security-1.0.pkg (For RaQ2 servers)
>
> http://www.cobaltnet.com/patches/RaQ2J-Security-1.0.pkg (For Japanese versions of the RaQ2 system)

The CERT/CC wishes to thank Cobalt Networks for their assistance in developing this advisory.

Revision History

```
Jul 30, 1999:   Initial release
Aug  8, 1999:   Updated link to Cobalt Networks announcement
Jul 25, 2001:   Fixed typo in title
```

11 CA-1999-11: Four Vulnerabilities in the Common Desktop Environment

Original release date: September 13, 1999
Last revised: March 02, 2000
Updated vendor information for Sun Microsystems, Inc.
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running the Common Desktop Environment (CDE)

I. Description

Multiple vulnerabilities have been identified in some distributions of the Common Desktop Environment (CDE). These vulnerabilities are different from those discussed in CA-98.02. We recommend that you install appropriate vendor patches as soon as possible (see Section III below). Until you can do so, we encourage you to disable or uninstall vulnerable copies of the CDE package. Note that disabling these programs will severely affect the utility of the CDE environment.

At this time, the CERT/CC has not received any reports of these vulnerabilities being exploited by intruders.

Vulnerability #1: ToolTalk *ttsession* uses weak RPC authentication mechanism

The ToolTalk messaging server *ttsession* allows independent applications to communicate without having direct knowledge of each other. Applications can communicate through an associated *ttsession* which delivers messages via RPC calls between interested agents.

On many systems, *ttsession* uses AUTH_UNIX authentication (a client-based security option) by default. When messages are received, *ttsession* uses certain environment variables supplied by the client to determine how the message is handled. Because of this, the *ttsession* process can be manipulated to execute unauthorized arbitrary programs with the privileges of the running ttsession.

Vulnerability #2: CDE *dtspcd* relies on file-system based authentication

The network daemon *dtspcd* (a CDE desktop subprocess control program) accepts CDE requests from clients to execute commands and launch applications remotely.

When a client makes a request, the *dtspcd* daemon asks the client to create a file that has a predictable name so that the daemon can authenticate the request. If a local user can manipulate the files used for authentication, then that user can craft arbitrary commands that may run as root.

Vulnerability #3: CDE *dtaction* buffer overflow

The *dtaction* utility allows applications or shell scripts that otherwise are not connected into the CDE development environment, to request that CDE actions be performed.

A buffer overflow can occur in some implementations of *dtaction* when a username argument greater than 1024 bytes is used.

Vulnerability #4: CDE ToolTalk shared library buffer overflow in TT_SESSION

There is a vulnerability in some implementations of the ToolTalk shared library which allows the TT_SESSION environment variable buffer to overflow. A setuid root program using a vulnerable ToolTalk library, such as *dtsession*, can be exploited to run arbitrary code as root.

II. Impact

Vulnerability #1: ToolTalk *ttsession* uses weak RPC authentication mechanism

A local or remote user may be able to use this vulnerability to run commands on a vulnerable system with the same privileges of the attacked *ttsession*. For this attack to work, a *ttsession* must be actively running on the system attacked. The *ttsession* daemon is started whenever a user logs in using the CDE desktop, or upon interaction with CDE at some future point.

Vulnerability #2: CDE *dtspcd* relies on file-system based authentication

A vulnerable *dtspcd* may allow a local user to run arbitrary commands as root.

Vulnerability #3: CDE *dtaction* buffer overflow

A local user may be able to exploit this vulnerability to execute arbitrary code with root privileges.

Vulnerability #4: CDE ToolTalk shared library buffer overflow in TT_SESSION

A local user may be able to exploit this vulnerability to execute arbitrary code with root privileges.

III. Solution

Install appropriate patches from your vendor

We recommend installing vendor patches as soon as possible and disabling the vulnerable programs until you can do so (or uninstalling the entire CDE package if not needed). Note that disabling these programs will severely affect the utility of the CDE environment.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Compaq Computer Corporation

Problem #1

CDE ToolTalk session daemon & ToolTalk shared library overflow

This potential security problem has been resolved and a patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E, V4.0F and V5.0.

This patch can be installed on:

```
V4.0D-F, all patch kits

V5.0, all patch kits
```

*This solution will be included in a future distributed release of Compaq's Tru64/ DIGITAL UNIX.

This patch may be obtained from the World Wide Web at the following FTP address: http://www.service.digital.com/patches.

The patch file name is **SSRT0617_ttsession.tar.Z**

Problem #2

Compaq's Tru64/DIGITAL UNIX is not vulnerable.

Problem #3

CDE dtaction buffer overflow

This potential security problem has been resolved and a patch for this problem has been made available for Tru64 UNIX V4.0D, V4.0E and V4.0F.

This patch can be installed on:

```
V4.0D Patch kit BL11 or BL12

V4.0E Patch kit BL1 or BL12

V4.0F Patch kit BL1
```

*This solution will be included in a future distributed release of Compaq's Tru64/ DIGITAL UNIX.

This patch may be obtained from the World Wide Web at the following FTP address: http://www.service.digital.com/patches.

The patch file name is **SSRT0615U_dtaction.tar.Z**

Problem #4

CDE ToolTalk shared library overflow

See solution fix described in in Problem #1.

Data General

DG/UX is not subject to any of these vulnerabilities.

Fujitsu

Fujitsu's UXP/V operating system is not vulnerable to any of these vulnerabilities.

Hewlett-Packard Company

HP-9000 Series 700/800 HP-UX releases 10.X and 11.0 systems with CDE patches previously recommended in HP Security Bulletins are not vulnerable to vulnerabilities #2, #3, and #4.

All HP-UX 10.X and 11.0 systems running CDE are vulnerable to vulnerability #1.

Patches are in progress.

IBM Corporation

All releases of AIX version 4 are vulnerable to vulnerabilities #1, #3, and #4. AIX is not vulnerable to #2. The following APARs will be available soon:

```
AIX 4.1.x:  IY03125  IY03847

AIX 4.2.x:  IY03105  IY03848

AIX 4.3.x:  IY02944  IY03849
```

Customers that do not require the CDE desktop functionality can disable CDE by restricting access to the CDE daemons and removing the **dt** entry from /etc/inittab. Run the following commands as root to disable CDE:

```
# /usr/dt/bin/dtconfig -d

# chsubserver -d -v dtspc

# chsubserver -d -v ttdbserver

# chsubserver -d -v cmsd

# chown root.system /usr/dt/bin/*

# chmod 0 /usr/dt/bin/*
```

For customers that require the CDE desktop functionality, a temporary fix is available via anonymous ftp from:
ftp://aix.software.ibm.com/aix/efixes/security/cdecert.tar.Z.

```
Filename        sum             md5

================================================================

dtaction_4.1    32885    18     82af470bbbd334b240e874ff6745d8ca

dtaction_4.2    52162    18     b10f21abf55afc461882183fbd30e602

dtaction_4.3    56550    19     6bde84b975db2506ab0cbf9906c275ed

libtt.a_4.1     29234  2132     f5d5a59956deb8b1e8b3a14e94507152

libtt.a_4.2     21934  2132     73f32a73873caff06057db17552b8560

libtt.a_4.3     12154  2118     b0d14b9fe4a483333d64d7fd695f084d

ttauth          56348    31     495828ea74ec4c8f012efc2a9e6fa731

ttsession_4.1   19528   337     bfac4a06b90cbccc0cd494a44bd0ebc9

ttsession_4.2   46431   338     05949a483c4e390403055ff6961b0816

ttsession_4.3   54031   339     e1338b3167c7edf899a33520a3adb060
```

NOTE - This temporary fix has not been fully regression tested. Use the following steps (as root) to install the temporary fix.

1. Uncompress and extract the fix.

```
# uncompress < cdecert.tar.Z | tar xf -

# cd cdecert
```

2. Replace the vulnerable executables with the temporary fix for your version of AIX.

```
# (cd /usr/dt/lib && mv libtt.a libtt.a.before_security_fix)

# (cd /usr/dt/bin && mv ttsession ttsession.before_security_fix)

# (cd /usr/dt/bin && mv dtaction dtaction.before_security_fix)

# chown root.system /usr/dt/lib/libtt.a.before_security_fix

# chown root.system /usr/dt/bin/ttsession.before_security_fix

# chown root.system /usr/dt/bin/dtaction.before_security_fix

# chmod 0 /usr/dt/lib/libtt.a.before_security_fix
```

```
# chmod 0 /usr/dt/bin/ttsession.before_security_fix

# chmod 0 /usr/dt/bin/dtaction.before_security_fix

# cp ./libtt.a_ /usr/dt/lib/libtt.a

# cp ./ttsession_ /usr/dt/bin/ttsession

# cp ./dtaction_ /usr/dt/bin/dtaction

# cp ./ttauth /usr/dt/bin/ttauth

# chmod 555 /usr/dt/lib/libtt.a

# chmod 555 /usr/dt/bin/ttsession

# chmod 555 /usr/dt/bin/dtaction

# chmod 555 /usr/dt/bin/ttauth
```

IBM AIX APARs may be ordered using Electronic Fix Distribution (via the FixDist program), or from the IBM Support Center. For more information on FixDist, and to obtain fixes via the Internet, please reference http://techsupport.services.ibm.com/support/rs6000.support/downloads or send electronic mail to aixserv@austin.ibm.com with the word "FixDist" in the "Subject:" line. To facilitate ease of ordering all security related APARs for each AIX release, security fixes are periodically bundled into a cumulative APAR. For more information on these cumulative APARs including last update and list of individual fixes, send electronic mail to aixserv@austin.ibm.com with the words "subscribe Security_APARs" in the "Subject:" line.

Santa Cruz Operation, Inc.

SCO is investigating these vulnerabilities on SCO UnixWare 7. Other SCO products (OpenServer 5.0.x, UnixWare 2.1.x, Open Server / Open Desktop 3.0 and CMW+) are not vulnerable as CDE is not a component of these releases.

SCO will make patches and status information available at http://www.sco.com/security.

Silicon Graphics, Inc.

SGI acknowledges the CDE vulnerabilities reported and is currently investigating. No further information is available at this time. As further information becomes available, additional advisories will be issued via the normal SGI security information distribution methods including the wiretap mailing list.

Until SGI has more definitive information to provide, customers are encouraged to assume all security vulnerabilities as exploitable and take appropriate steps according to local site security policies and requirements.

The SGI Security Headquarters Web page is accessible at the URL

http://www.sgi.com/Support/security/security.html

Sun Microsystems, Inc.

Please see Sun Security Bulletin #00192: CDE and OpenWindows at http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/192&type=0&nav=sec.sba

The CERT Coordination Center would like to thank Job de Haas for reporting these vulnerabilities and working with the vendors to effect fixes. We would also like to thank Solutions Atlantic for their efforts in coordinating vendor solutions.

Revision History

```
Mar  02, 2000:  Updated vendor information for Sun Microsystems, Inc.

Oct  04, 1999:  Updated vendor information for Sun Microsystems, Inc.

Oct  01, 1999:  Added vendor information for Data General

Sep  13, 1999:  Initial release
```

12 CA-1999-12: Buffer Overflow in amd

Original release date: September 16, 1999
Last revised: --
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running *amd*, the Berkeley Automounter Daemon

I. Description

There is a buffer overflow vulnerability in the logging facility of the *amd* daemon.

This daemon automatically mounts file systems in response to attempts to access files that reside on those file systems. Similar functionality on some systems is provided by a daemon named *automountd*.

Systems that include automounter daemons based on BSD 4.x source code may also be vulnerable. A vulnerable implementation of *amd* is included in the am-utils package, provided with many Linux distributions.

II. Impact

Remote intruders can execute arbitrary code as the user running the *amd* daemon (usually root).

III. Solution

Install a patch from your vendor

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

We will update this advisory as more information becomes available. Please check the CERT/CC Web site for the most current revision.

Disable amd

If you are unable to apply a patch for this problem, you can disable the *amd* daemon to prevent this vulnerability from being exploited. Disabling *amd* may prevent your system from operating normally.

Appendix A. Vendor Information

BSDI

BSD/OS 4.0.1 and 3.1 are both vulnerable to this problem if amd has been configured. The amd daemon is not started if it has not been configured locally. Mods (M410-017 for 4.0.1 and M310-057) are available via ftp from ftp://ftp.bsdi.com/bsdi/patches or via our web site at http://www.bsdi.com/support/patches

Compaq Computer Corporation

Not vulnerable

Data General

DG/UX is not vulnerable to this problem.

Erez Zadok (am-utils maintainer)

The latest stable version of am-utils includes several important security fixes. To retrieve it, use anonymous ftp for the following URL: ftp://shekel.mcl.cs.columbia.edu/pub/am-utils/.

The MD5 checksum of the am-utils-6.0.1.tar.gz archive is
MD5 (am-utils-6.0.1.tar.gz) = ac33a4394d30efb4ca47880cc5703999

The simplest instructions to build, install, and run am-utils are as follows:

1. Retrieve the package via FTP.
2. Unpack it:

   $ gunzip am-utils-6.0.1.tar.gz
   $ tar xf am-utils-6.0.1.tar

   If you have GNU tar and gunzip, you can issue a single command:

   $ tar xzf am-utils-6.0.1.tar.gz

3. Build it:

   $ cd am-utils-6.0.1
   $ ./buildall

   This would configure and build am-utils for installation in /usr/local. If you built am-utils in the past using a different procedure, you may repeat that procedure instead. For example, to build am-utils using shared libraries and to enable debugging, use either:

   $ ./buildall -Ds -b
   or
   $ ./configure --enable-debug=yes --enable-shared --disable-static

   You may run "./configure --help" to get a full list of available options. You may run "./buildall -H" to get a full list of options it offers. The buildall script is a simple wrapper script that configures and builds am-utils for the most common desired configurations.

4. Install it:

   $ make install

   This would install the programs, scripts, libraries, manual pages, and info pages in /usr/local/{sbin,bin,lib,man,info}, etc.

5. Run it.

   Assuming you have an Amd configuration file in /etc/amd.conf, you can simply run:

   $ /usr/local/sbin/ctl-amd restart

   That will stop the older running Amd, and start a new one. If you use a different Amd start-up script, you may use it instead.

FreeBSD

Please see the FreeBSD advisory at
ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-99:06.amd.asc.

for i.nformation on patches for this problem.

Fujitsu

This vulnerability is still under investigation by Fujitsu.

Hewlett-Packard Company

HP is not vulnerable.

IBM Corporation

AIX is not vulnerable. It does not ship the am-utils package.

OpenBSD

OpenBSD is not vulnerable.

RedHat Inc.

RedHat has released a security advisory on this topic. It is available from our ftp server at:
http://www.redhat.com/corp/support/errata/RHSA1999032_O1.html.

SCO Unix

No SCO products are vulnerable.

SGI

SGI does not distribute am-utils in either IRIX or UNICOS operating systems.

Sun Microsystems, Inc.

SunOS - All versions are not vulnerable.

Solaris - All versions are not vulnerable.

The CERT Coordination Center would like to thank Erez Zadok, the maintainer of the am-utils package, for his assistance in preparing this advisory.

Revision History

```
Sep 16, 1999:  Initial release
```

13 CA-1999-13: Multiple Vulnerabilities in WU-FTPD

Original release date: October 19, 1999
Last revised: November 9, 1999
Added vendor information for Fujitsu.
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running the WU-FTPD daemon or its derivatives

I. Description

Three vulnerabilities have been identified in WU-FTPD and other ftp daemons based on the WU-FTPD source code. WU-FTPD is a common package used to provide File Transfer Protocol (FTP) services. Incidents involving at least the first of these vulnerabilities have been reported to the CERT Coordination Center.

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

Because of improper bounds checking, it is possible for an intruder to overwrite static memory in certain configurations of the WU-FTPD daemon. The overflow occurs in the MAPPING_CHDIR portion of the source code and is caused by creating directories with carefully chosen names. As a result, FTP daemons compiled without the MAPPING_CHDIR option are not vulnerable.

This is the same vulnerability described in AUSCERT Advisory AA-1999.01, which is available from ftp://www.auscert.org.au/security/advisory/AA-1999.01.wu-ftpd.mapping_chdir.vul.

This is not the same vulnerability as the one described in CA-99-03 "FTP Buffer Overflows", even though it is closely related. Systems that have patches to correct the issue described in CA-99-03 may still be vulnerable to this problem.

Vulnerability #2: Message File Buffer Overflow

Because of improper bounds checking during the expansion of macro variables in the message file, intruders may be able to overwrite the stack of the FTP daemon.

This is one of the vulnerabilities described in AUSCERT Advisory AA-1999.02, which is available from ftp://www.auscert.org.au/security/advisory/AA-1999.02.multi.wu-ftpd.vuls.

Vulnerability #3: SITE NEWER Consumes Memory

The SITE NEWER command is a feature specific to WUFTPD designed to allow mirroring software to identify all files newer than a supplied date. This command fails to free memory under some circumstances.

II. Impact

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

Remote and local intruders may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

To exploit this vulnerability, the intruder must be able to create directories on the vulnerable systems that are accessible via FTP. While remote intruders are likely to have this privilege only through anonymous FTP access, local users may be able to create the required directories in their own home directories.

Vulnerability #2: Message File Buffer Overflow

Remote and local intruders may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

If intruders are able to control the contents of a message file, they can successfully exploit this vulnerability. This access is frequently available to local users in their home directories, but it may be restricted in anonymous FTP access, depending on your configuration.

Additionally, under some circumstances, remote intruders may be able to take advantage of message files containing macros provided by the FTP administrator.

Vulnerability #3: SITE NEWER Consumes Memory

Remote and local intruders who can connect to the FTP server can cause the server to consume excessive amounts of memory, preventing normal system operation. If intruders can create files on the system, they may be able exploit this vulnerability to execute arbitrary code as the user running the ftpd daemon, usually root.

III. Solution

Install appropriate patches from your vendor

These vulnerabilities can be eliminated by applying appropriate patches from your vendor. We encourage you to apply a patch as soon as possible and to disable vulnerable programs until you can do so.

Disabling the WU-FTPD daemon may prevent your system from operating normally. Upgrading to WU-FTPD 2.6.0 may cause some inter-operability problems with certain FTP clients. We encourage you to review the WU-FTPD documentation carefully before performing this upgrade.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Until you can install a patch, you can apply the following workarounds.

Vulnerability #1: MAPPING_CHDIR Buffer Overflow

This vulnerability can be corrected by compiling the WU-FTPD daemon without the MAPPING_CHDIR option. Exploitation by anonymous remote intruders can be mitigated by limiting write access, but this solution is not encouraged.

Vulnerability #2: Message File Buffer Overflow

Remote exploitation of this vulnerability can be mitigated and possibly eliminated by removing macros from message files until a patch can be applied.

Vulnerability #3: SITE NEWER Consumes Memory

There are currently no workarounds available.

Appendix A Vendor Information

Data General

DG/UX is not vulnerable to this problem.

FreeBSD

FreeBSD has updated its wuftpd and proftpd ports to correct this problem as of August 30, 1999. Users of these ports are encouraged to upgrade their installation to these newer versions of these ports as soon as possible.

Fujitsu

The Fujitsu UXP/V Operating System is not vulnerable.

IBM Corporation

AIX is not vulnerable. It does not ship wu-ftpd.

IBM and AIX are registered trademarks of International Business Machines Corporation.

OpenBSD

OpenBSD does not use (and never will use) wuftpd or any of its derivatives.

Santa Cruz Operation, Inc.

Security patches for SCO UnixWare 7.x, SCO UnixWare 2.x, and OpenServer 5.x will be made available at http://www.sco.com/security.

SGI

SGI IRIX and Unicos do not ship with wu-ftpd, so they are not vulnerable. As a courtesy, unsupported pre-compiled IRIX inst images for wu-ftpd are available from http://freeware.sgi.com/ which may be vulnerable. When the freeware products are next updated, they should contain the latest wu-ftpd code which should include the security fixes.

SGI Linux 1.0 which is based on RedHat 6.0 ships with wu-ftpd rpms. When new wu-ftpd rpms are available for RedHat 6.0, they can be installed on SGI Linux 1.0.

SGI NT Workstations do not ship with wu-ftpd.

Sun

Sun is not vulnerable.

WU-FTPD and BeroFTPD

Vulnerability #1:

> Not vulnerable:
> versions 2.4.2 and all betas and earlier versions
>
> Vulnerable:
> wu-ftpd-2.4.2-beta-18-vr4 through wu-ftpd-2.4.2-beta-18-vr15
> wu-ftpd-2.4.2-vr16 and wu-ftpd-2.4.2-vr17
> wu-ftpd-2.5.0
> BeroFTPD, all versions

Vulnerability #2:

> Not vulnerable:
> wu-ftpd-2.6.0
>
> Vulnerable:
> All versions of wuarchive-ftpd and wu-ftpd prior to version 2.6.0, from wustl.edu, academ.com, vr.net and wu-ftpd.org.
> BeroFTPD, all versions

Vulnerability #3:

> Not vulnerable:
> wu-ftpd-2.6.0
>
> Vulnerable:
> All versions of wuarchive-ftpd and wu-ftpd prior to version 2.6.0, from wustl.edu, academ.com, vr.net and wu-ftpd.org.
> BeroFTPD, all versions

With version 2.6.0, the major functionality of BeroFTPD has been merged back into the WU-FTPD daemon. Development of BeroFTPD has ceased; there will be no upgrades or patches. Users are advised to upgrade to WU-FTPD version 2.6.0.

WU-FTPD Version 2.6.0 is available for download from mirrors arround the world. A full list of mirrors is available from: ftp://ftp.wu-ftpd.org/pub/README-MIRRORS.

The current version of WU-FTPD (presently 2.6.0) is also available from the primary distribution site:

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-current.tar.gz

ftp://ftp.wu-ftpd.org/pub/wu-ftpd/wu-ftpd-current.tar.Z

The CERT Coordination Center would like to thank Gregory Lundberg (a member of the WU-FTPD development group) and AUSCERT their assistance in preparing this advisory.

Revision History

```
October 19, 1999  Initial release

November 9, 1999  Added vendor information for Fujitsu.
```

14 CA-1999-14: Multiple Vulnerabilities in BIND

Original release date: November 10, 1999
Last revised: April 25, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running various versions of BIND

I. Description

Six vulnerabilities have been found in BIND, the popular domain name server from the Internet Software Consortium (ISC). One of these vulnerabilities may allow remote intruders to gain privileged access to name servers.

Vulnerability #1: the "nxt bug"

Some versions of BIND fail to properly validate NXT records. This improper validation could allow an intruder to overflow a buffer and execute arbitrary code with the privileges of the name server.

NXT record support was introduced in BIND version 8.2. Prior versions of BIND, including 4.x, are not vulnerable to this problem. The ISC-supplied version of BIND corrected this problem in version 8.2.2.

Vulnerability #2: the "sig bug"

This vulnerability involves a failure to properly validate SIG records, allowing a remote intruder to crash *named*; see the impact section for additional details.

SIG record support is found in multiple versions of BIND, including 4.9.5 through 8.x.

Vulnerability #3: the "so_linger bug"

By intentionally violating the expected protocols for closing a TCP session, remote intruders can cause *named* to pause for periods up to 120 seconds.

Vulnerability #4: the "fdmax bug"

Remote intruders can consume more file descriptors than BIND can properly manage, causing *named* to crash.

Vulnerability #5: the "maxdname bug"

Improper handling of certain data copied from the network could allow a remote intruder to disrupt the normal operation of your name server, possibly including a crash.

Vulnerability #6: the "naptr bug"

Some versions of BIND fail to validate zone information loaded from disk files. In environments with unusual combinations of permissions and protections, this could allow an intruder to crash *named*.

Other recent BIND-related vulnerabilities

AusCERT recently published a report describing denial-of-service attacks against name servers. These attacks are unrelated to the issues described in this advisory. For information on the denial-of-service attacks described by AusCERT, please see AusCERT Alert AL-1999.004 available at: ftp://ftp.auscert.org.au/pub/auscert/advisory/AL-1999.004.dns_dos.

II. Impact

Vulnerability #1

By exploiting this vulnerability, remote intruders can execute arbitrary code with the privileges of the user running *named*, typically root.

Vulnerabilities #2, #4, and #5

By exploiting these vulnerabilities, remote intruders can disrupt the normal operation of your name server, possibly causing a crash.

Vulnerability #3

By periodically exercising this vulnerability, remote intruders can disrupt the ability of your name server to respond to legitimate queries. By intermittently exercising this vulnerability, intruders can seriously degrade the performance of your name server.

Vulnerability #6

Local intruders who gain write access to your zone files can cause *named* to crash.

III. Solution

Apply a patch from your vendor or update to a later version of BIND

Many operating system vendors distribute BIND with their operating system. Depending on your support procedures, arrangements, and contracts, you may wish to obtain BIND from your operating system vendor rather than directly from ISC.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive more information. If you do not see your vendor's name, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Vendor Name

Caldera

See ftp://ftp.calderasystems.com/pub/OpenLinux/updates/2.3/current.

MD5s

```
db1dda05dbe0f67c2bd2e5049096b42c  RPMS/bind-8.2.2p3-1.i386.rpm

82bbe025ac091831904c71c885071db1  RPMS/bind-doc-8.2.2p3-1.i386.rpm

2f9a30444046af551eafd8e6238a50c6  RPMS/bind-utils-8.2.2p3-1.i386.rpm

0e4f041549bdd798cb505c82a8911198  SRPMS/bind-8.2.2p3-1.src.rpm
```

Compaq Computer Corporation

At the time of writing this document, Compaq is currently investigating the potential impact to Compaq's BIND release(s).

As further information becomes available Compaq will provide notice of the completion/availability of any necessary patches through AES services (DIA, DSNlink FLASH and posted to the Services WEB page) and be available from your normal Compaq Services Support channel.

Data General

We are investigating. We will provide an update when our investigation is complete.

Hewlett-Packard Company

HP is vulnerable, see the chart in the ISC advisory for details on your installed version of BIND. Our fix strategy is under investigation, watch for updates to this CERT advisory in the CERT archives, or an HP security advisory/bulletin.

IBM Corporation

The bind8 shipped with AIX 4.3.x is vulnerable. We are currently working on the following APARs which will be available soon: APAR 4.3.x: IY05851

To Order

APARs may be ordered using Electronic Fix Distribution (via FixDist) or from the IBM Support Center. For more information on FixDist, reference URL:

http://aix.software.ibm.com/aix.us/swfixes/ or send e-mail to aixserv@austin.ibm.com with a subject of "FixDist".

IBM and AIX are registered trademarks of International Business Machines Corporation.

C

ISC has published an advisory regarding these problems, available at http://www.isc.org/products/BIND/bind-security-19991108.html.

The ISC advisory also includes a table summarizing which versions of BIND are susceptible to the vulnerabilities described in this advisory.

OpenBSD

As far as we know, we don't ship with any of those vulnerabilities.

Santa Cruz Operation, Inc

Security patches for the following SCO products will be made available at http://www.sco.com/security.

OpenServer 5.x.x, UnixWare 7.x.x, UnixWare 2.x.x

Sun Microsystems

Please see updated information at: Sun Microsystems, Inc. Security Bulletin #00194: BIND.

Vulnerability #1

> Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, and 7 are not vulnerable.

Vulnerability #2

> Solaris 2.3, 2.4, 2.5, 2.5.1, 2.6, and 7 are not vulnerable.

For Vulnerabilities #3, #4, #5, and #6:

> Solaris 2.3, 2.4, 2.5, 2.5.1, and 2.6 are not vulnerable.
> Sun has produced the following patches for Solaris 7.

Solaris version	Patch ID
Solaris 7 (SPARC)	107018-02
	106938-03
Solaris 7 (Intel)	107019-02
	106939-03

The CERT Coordination Center would like to thank David Conrad, Paul Vixie and Bob Halley of the Internet Software Consortium for notifying us of these problems and for their help in constructing the advisory, and Olaf Kirch of Caldera for notifying us of some of these problems and providing technical assistance and advice.

Revision History

November 10, 1999:	Initial release
April 25, 2000:	Updated vendor information for Sun

15 CA-1999-15: Buffer Overflows in SSH daemon and RSAREF2 Library

Original release date: December 13, 1999
Last revised: March 3, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems running some versions of sshd
- Systems using products that use RSAREF2 (e.g., some SSL-enabled web servers)

I. Description

Some versions of sshd are vulnerable to a buffer overflow that can allow an intruder to influence certain variables internal to the program. This vulnerability alone does not allow an intruder to execute code.

However, a vulnerability in RSAREF2, which was discovered and researched by Core SDI, can be used in conjunction with the vulnerability in sshd to allow a remote intruder to execute arbitrary code.

Additional information about the RSAREF2 vulnerability can be found at http://www.core-sdi.com/advisories/buffer%20overflow%20ing.htm.

The RSAREF2 library was developed from a different code base than other implementations of the RSA algorithm, including those from RSA Security Inc. The vulnerability described in this advisory is specific to the RSAREF2 library and does not imply any weakness in other implementations of the RSA algorithm or the algorithm itself.

Also, only versions of SSH compiled with RSAREF support, via the *--with-rsaref* option, are vulnerable to these issues.

The use of the RSAREF2 library in other products may present additional vulnerabilities. RSAREF2 may be used in products such as SSL-enabled web servers, ssh clients, or other cryptographically enhanced products. Appendix A of this advisory will be updated with new information as it becomes available regarding problems in other products that use the RSAREF2 library.

II. Impact

Using the two vulnerabilities in conjunction allows an intruder to execute arbitrary code with the privileges of the process running sshd, typically root.

We are investigating whether vulnerabilities in other products may expose the vulnerability in RSAREF2, and will update this advisory as appropriate.

See Appendices A and B for more information that may affect the impact of this vulnerability.

III. Solution

Apply patch(es) from your product vendor

Apply patch(es) to the RSAREF2 library. RSA Security Inc. holds a patent on the RSA algorithm and a copyright on the RSAREF2 implementation. We encourage you to consult your legal counsel regarding the legality of any fixes you are considering before implementing those fixes. Please see RSA's vendor statement in Appendix A.

Exploiting the vulnerability in RSAREF2 requires an application program to call the RSAREF2 library with malicious input. For products that allow an intruder to influence the data provided to the RSAREF2 library, you may be able to protect against attacks by validating the data they provide to RSAREF2.

Appendix A contains information provided by vendors for this advisory. Appendix B contains information regarding tests performed by the CERT Coordination Center and other people, and advice based on those tests. We will update the appendices as we receive or develop more information. If you do not see your vendor's name in Appendix A, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Use a non-vulnerable implementation of the RSA algorithm

Sites not restricted by patent law may choose to use a non-vulnerable implementation of RSA. Since RSA Security Inc. holds a patent on the RSA algorithm, this option may not be legally available to you. Please consult your legal counsel for guidance on this issue.

Appendix A Vendor Information

Compaq Computer Corporation

SOURCE:

> Compaq Computer Corporation
> Compaq Services
> Software Security Response Team USA

Compaq's Tru64 UNIX is not vulnerable. Compaq does not ship ssl

Covalent Technologies

Covalent Raven SSL module for Apache

The Raven SSL module is not vulnerable to this attack since the SSL library used does not use the RSAREF library.

Data Fellows Inc.

F-Secure SSH versions prior 1.3.7 are vulnerable but F-Secure SSH 2.x and above are not.

FreeBSD

FreeBSD 3.3R and prior releases contain packages with this problem. This problem was corrected December 2, 1999 in the ports tree. Packages built after this date with the rsaref updated should be unaffected by this vulnerabilities. Some or all of the following ports may be affected should be rebuilt:

> p5-Penguin, p5-Penguin-Easy, jp-pgp, ja-w3m-ssl, ko-pgp, pgpsendmail, pine4-ssl, premail, ParMetis, SSLtelnet, mpich, pipsecd, tund, nntpcache, p5-Gateway, p5-News-Article, ru-pgp, bjorb, keynote, OpenSSH, openssl, p5-PGP, p5-PGP-Sign, pgp, slush, ssh, sslproxy, stunnel, apache+mod_ssl, apache+ssl, lynx-ssl, w3m-ssl, zope

Please see the FreeBSD Handbook for information on how to obtain a current copy of the ports tree and how to rebuild those ports which depend on rsaref.

Fujitsu

Fujitsu's UXP/V operating system does not support secure shell (SSH). Therefore, it is not vulnerable to this problem.

Hewlett-Packard Company

HP does not supply SSH. HP has not conducted compatibility testing with version 1.2.27 of SSH, when compiled with the option *--with-rsaref*. Further, RSAREF2 has not been tested to date. As far as the investigation to date, HP appears to be not vulnerable.

IBM Corporation

IBM AIX does not currently ship the secure shell (ssh) nor do the base components of AIX ship or link with the RSAREF2 library.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Microsoft

The Microsoft Security Response Team has investigated this issue, and no Microsoft products are affected by the vulnerability.

NetBSD

NetBSD does not ship with ssh in either its US-only or International variants at this time, so no default installation of NetBSD is vulnerable.

However, ssh is installed and widely used by many NetBSD installations, and is available from our software package tree in source form. The NetBSD ssh package can be compiled either with or without RSAREF2, settable by the administrator at compile time according to local copyright and license restrictions.

Installations which used RSAREF2 in compiling ssh are vulnerable, and we recommend recompiling without RSAREF2 if their local legal situation permits.

In addition, the following list of software packages in the NetBSD "packages" system are also dependent on the RSAREF2 library:

- archivers/hpack
- security/openssl
- security/pgp2
- security/pgp5
- www/ap-ssl

of those, the security/openssl package is itself a library, and the following packages depend on it:

- net/ppp-mppe
- net/speakfreely-crypto
- www/ap-ssl

We recommend recompiling and reinstalling these packages without RSAREF2, if your local legal situation permits.

Network Associates, Inc.

After a technical review of the buffer overflow bug in RSAREF, we have determined at Network Associates that PGP is not affected by this bug, because of the careful way that PGP uses RSAREF.

This applies to all versions of PGP ever released by MIT, which are the only versions of PGP that use RSAREF. All other versions of PGP, such as the commercial versions and the international versions, avoid the use of RSAREF entirely.

Philip Zimmermann
10 December 1999

[CERT/CC Note: A PGP signed copy of this information and additional technical details are available as well.]

OpenSSL

OpenSSL with RSAREF is not vulnerable.

OpenBSD / OpenSSH

More information is available from: http://www.openbsd.org/errata.html#sslUSA.

RSA Security Inc.

RSA Security Inc. recommends that developers implement the proposed or similar patch to RSAREF version 2.0 or otherwise to ensure that the length in bits of the modulus supplied to RSAREF is less than or equal to MAX_RSA_MODULUS_BITS.

RSA Security Inc. is no longer distributing the RSAREF toolkit, which it offered through RSA Laboratories in the mid-1990s as a free, source implementation of modern cryptographic algorithms. Under the terms of the RSAREF license, changes to the RSAREF code other than porting or performance improvement require written consent. RSA Security hereby gives its consent to implement a patch to RSAREF to address this advisory.

This advisory only applies to RSAREF, not RSA Security's current toolkits and products, which were developed independently of RSAREF.

Although RSA Security is no longer distributing RSAREF, the toolkit is still available in a number of "freeware" products such as SSH under RSA Security's original RSAREF v2.0 software license ("license.txt", March 25, 1994), which is distributed along with those products. As a reminder, that license limits the use of RSAREF to noncommercial purposes. RSAREF, RSAREF applications, and services based on RSAREF applications may not be sold, licensed or otherwise transferred for value. (There is a minor exception for small "shareware" deployments as noted in the "info.txt" file, March 25, 1994.)

SSH Communications

The bug only affects ssh when it is compiled with RSAREF (i.e., only when --with-rsaref is explicitly supplied on the command line). Any version compiled without --with-rsaref is not affected. The problem should not affect users of the commercial versions (who are licensed to use the built-in RSA) or users outside the United States (who are presumably not using RSAREF and can use the built-in RSA without needing a license). I.e., only those non-commercial users who actually compile with a separately obtained RSAREF should be affected.

The bug is present in all versions of SSH1, up to and including 1.2.27. It will be fixed in ssh-1-2.28 (expected to go out in a few days to fix this problem). It does not affect SSH2. (Please note that ssh1 is no longer maintained, except for security fixes, due to certain rather fundamental problems that have been fixed in ssh2.)

Any implementation compiled without an explicitly specified --with-rsaref is not affected by this problem.

A patch provided by SSH Communications is available from the CERT/CC web site. This version of the patch has been signed by the CERT/CC.

Stronghold

Stronghold does not use RSAREF and is unaffected.

Appendix B CERT/CC and Other Third-Party Tests

RSAREF Patch from Core SDI and the CERT/CC

With the assistance of Core SDI, the CERT Coordination Center tested sshd version 1.2.27 running on an Intel-based RedHat Linux system and found that configuration to be vulnerable. Tests conducted by Core SDI indicate that sshd 1.2.27 running on OpenBSD and FreeBSD on Intel is also vulnerable, and it is likely that other configurations are vulnerable as well.

CERT/CC has developed a patch for the RSAREF2 vulnerability based in part on work done by Core SDI. This patch is available at

ftp://ftp.core-sdi.com/pub/patches/rsaref2.patch

http://www.cert.org/advisories/CA-99-15/rsa-patch.txt

You can verify this patch with a detached PGP signature from the CERT/CC.

This patch should be applied to the rsa.c source file that comes with the RSAREF distribution. Note that there is also an rsa.c source file that is part of the SSH distribution, and that this patch will not apply correctly to that file. When in the correct directory (the RSAREF source directory) the patch can be applied by issuing the command:

```
patch <rsa-patch.txt
```

We believe the patch *originally* provided by Core SDI in their advisory may not be a complete fix to this particular problem. We have worked with them to develop an updated patch and gratefully acknowledge their contribution to the fix provided here. Neither the CERT/CC, the Software Engineering Institute, nor Carnegie Mellon University provides any warranties regarding this patch. Please see our disclaimer at the end of this advisory.

Possible vulnerability of ssh clients

The possible vulnerability of ssh clients is of particular concern. As we learn more regarding the vulnerability of ssh clients, we will update this advisory. One possible way to attack an ssh client would be to construct a malicious ssh server and lure or trick victims into connecting to the server. The ssh client will warn users when it connects to a site that presents a key that does not match one previously associated with the server. The dialog may be similar to the following:

```
% ssh badhost

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@       WARNING: HOST IDENTIFICATION HAS CHANGED!         @

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle
attack)!

It is also possible that the host key has just been changed.

Please contact your system administrator.

Add correct host key in /etc/.ssh/known_hosts to get rid of this
message.

Are you sure you want to continue connecting (yes/no)? no

%
```

If you see this warning, you should answer "no" to the prompt and investigate why the key you received does not match the key you expected.

The CERT Coordination Center would like to thank Alberto Solino <Alberto_Solino@core-sdi.com> and Gerardo Richarte <Gerardo_Richarte@core-sdi.com> of Core SDI S.A. Seguridad de la informacion, Buenos Aires, Argentina (http://www.core-sdi.com), who discovered the problem in RSAREF2 and provided valuable technical assistance. We would also like to thank Andrew Cormack of JANET CERT, who provided technical assistance; Theo de Raadt of the OpenBSD project, who provided valuable feedback used in the construction of this advisory; Burt Kaliski of RSA Security Inc.; and Tatu Ylonen of SSH Communications Security.

Revision History

```
December 13, 1999:  Initial release

March 3, 2000: Clarified how to apply RSAREF patch
```

16 CA-1999-16: Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind

Original release date: December 14, 1999
Last revised: March 02, 2000
Updated vendor information for Sun
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- Systems that have *sadmind* installed

I. Description

The *sadmind* program is installed by default in Solaris 2.5, 2.5.1, 2.6, and 7. In Solaris 2.3 and 2.4, sadmind may be installed if the Sun Solstice Adminsuite packages are installed. The sadmind program is installed in /usr/sbin. It can be used to coordinate distributed system administration operations remotely. The *sadmind* daemon is started automatically by the *inetd* daemon whenever a request to perform a system administration operation is received.

All versions of *sadmind* are vulnerable to a buffer overflow that can overwrite the stack pointer within a running *sadmind* process. Since *sadmind* is installed as root, it is possible to execute arbitrary code with root privileges on a remote machine.

This vulnerability has been discussed in public security forums and is actively being exploited by intruders.

II. Impact

A remote user may be able to execute arbitrary code with root privileges on systems running vulnerable versions of *sadmind*.

III. Solution

Apply Sun's recommended patches for *sadmind*

Please see Appendix A for more information.

Disable *sadmind*

Remove (or comment) the following line in **/etc/inetd.conf**:

```
100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind
```

Even though it will **not** defend against the attack discussed in this advisory, it is a good practice to set the security option used to authenticate requests to a STRONG level, for example:

```
100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind -S 2
```

If you must use *sadmind* to perform system administration tasks, we urge you to use this setting.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive or develop more information. If you do not see your vendor's name in Appendix A, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Sun Microsystems

Sun has published Sun Security Bulletin #00191 to address this issue:

http://sunsolve.sun.com/pub-cgi/retrieve.pl?doctype=coll&doc=secbull/191&type=0&nav=sec.sba

The CERT Coordination Center thanks Sun Microsystems for its help in providing information for this advisory.

Revision History

```
Mar 02, 2000:   Changed pointers to Sun Bulletin #00191 to public
pages

Jan 12, 1999:   Added updates from Sun, including Sun Security Bul-
letin #00191

Dec 16, 1999:   Added updates from Sun, including patch versions

Dec 14, 1999:   Initial release
```

17 CA-1999-17: Denial-of-Service Tools

Original release date: December 28, 1999
Last Updated: March 3, 2000
Source: CERT/CC

A complete revision history is at the end of this file.

Systems Affected

- All systems connected to the Internet can be affected by denial-of-service attacks. Tools that run on a variety of UNIX and UNIX-like systems and Windows NT systems have recently been released to facilitate denial-of-service attacks. Additionally, some MacOS systems can be used as traffic amplifiers to conduct a denial-of-service attack.

I. Description

New Distributed Denial-of-Service Tools

Recently, new techniques for executing denial-of-service attacks have been made public. A tool similar to Tribe FloodNet (TFN), called Tribe FloodNet 2K (TFN2K) was released. Tribe FloodNet is described in http://www.cert.org/incident_notes/IN-99-07.html#tfn.

Like TFN, TFN2K is designed to launch coordinated denial-of-service attacks from many sources against one or more targets simultaneously. It includes features designed specifically to make TFN2K traffic difficult to recognize and filter, to remotely execute commands, to obfuscate the true source of the traffic, to transport TFN2K traffic over multiple transport protocols including UDP, TCP, and ICMP, and features to confuse attempts to locate other nodes in a TFN2K network by sending "decoy" packets.

TFN2K is designed to work on various UNIX and UNIX-like systems and Windows NT.

TFN2K obfuscates the true source of attacks by spoofing IP addresses. In networks that employ ingress filtering as described in [1], TFN2K can forge packets that appear to come from neighboring machines.

Like TFN, TFN2K can flood networks by sending large amounts of data to the victim machine. Unlike TFN, TFN2K includes attacks designed to crash or introduce instabilities in systems by sending malformed or invalid packets. Some attacks like this are described in

http://www.cert.org/advisories/CA-98-13-tcp-denial-of-service.html

http://www.cert.org/advisories/CA-97.28.Teardrop_Land.html

Also like TFN, TFN2K uses a client-server architecture in which a single client, under the control of an attacker, issues commands simultaneously to a set of TFN2K servers. The servers then conduct the denial-of-service attacks against the victim(s). Installing the server requires that an intruder first compromise a machine by different means.

Asymmetric traffic from MacOS 9

MacOS 9 can be abused by an intruder to generate a large volume of traffic directed at a victim in response to a small amount of traffic produced by an intruder. This allows an intruder to use MacOS 9 as a "traffic amplifier," and flood victims with traffic. According to [3], an intruder can use this asymmetry to "amplify" traffic by a factor of approximately 37.5, thus enabling an intruder with limited bandwidth to flood a much larger connection. This is similar in effect and structure to a "smurf" attack, described in http://www.cert.org/advisories/CA-98.01.smurf.html.

Unlike a smurf attack, however, it is not necessary to use a directed broadcast to achieve traffic amplification.

II. Impact

Intruders can flood networks with overwhelming amounts of traffic or cause machines to crash or otherwise become unstable.

III. Solution

The problem of distributed denial-of-service attacks is discussed at length in [2], available at http://www.cert.org/reports/dsit_workshop.pdf.

Managers, system administrators, Internet Service Providers (ISPs) and Computer Security Incident Response Teams (CSIRTs) are encouraged to read this document to gain a broader understanding of the problem.

For the ultimate victim of distributed denial-of-service attacks

Preparation is crucial. The victim of a distributed denial-of-service attack has little recourse using currently available technology to respond to an attack in progress. According to [2]:

> *The impact upon your site and operations is dictated by the (in)security of other sites and the ability of of a remote attackers to implant the tools and subsequently to control and direct multiple systems worldwide to launch an attack.*

Sites are strongly encouraged to develop the relationships and capabilities described in [2] *before* you are a victim of a distributed denial-of-service attack.

For all Internet Sites

System and network administrators are strongly encouraged to follow the guidelines listed in [2]. In addition, sites are encouraged to implement ingress filtering as described in [1]. CERT/CC recommends implementing such filtering on as many routers as practical. This method is not foolproof, as mentioned in [1]:

> *While the filtering method discussed in this document does absolutely nothing to protect against flooding attacks which originate from valid prefixes (IP addresses), it will prohibit an attacker within the originating network from launching an attack of this nature using forged source addresses that do not conform to ingress filtering rules.*

Because TFN2K implements features designed specifically to take advantage of the granularity of ingress filtering rules, the method described in [1] means that sites may only be able to determine the network or subnet from which an attack originated.

Sites using manageable hubs or switches that can track which IP addresses have been seen at a particular port or which can restrict which MAC addresses can be used on a particular port may be able to further identify which machine(s) is responsible for TFN2K traffic. For further information, consult the documentation for your particular hub or switch.

The widespread use of this type of filtering can significantly reduce the ability of intruders to use spoofed packets to compromise or disrupt systems.

Preventing your site from being used by intruders

TFN2K and similar tools rely on the ability of intruders to install the client. Preventing your system from being used to install the client will help prevent intruders from using your systems to launch denial-of-service attacks (in addition to whatever damage they may cause to your systems).

Sites are encouraged to regularly visit this page and address any issues found there.

For the "Mac Attack"

Apple has developed a patch, as described in Appendix A. Please see the information there.

Appendix A contains information provided by vendors for this advisory. We will update the appendix as we receive or develop more information. If you do not see your vendor's name in Appendix A, the CERT/CC did not hear from that vendor. Please contact your vendor directly.

Appendix A Vendor Information

Apple Computer

OT Tuner 1.0 switches off an option in Open Transport that would cause a Macintosh to respond to certain small network packets with a large Internet Control Message Protocol (ICMP) packet. This update prevents Macintosh computers from being the cause of certain types of Denial of Service (DOS) issues.

The update is available from our software update server at http://asu.info.apple.com/swupdates.nsf/artnum/n11560.

In addition, it will soon be available via the automatic update feature that is part of Mac OS 9.

References

[1] RFC2267, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing , P. Ferguson, D. Senie, The Internet Society, January, 1998, available at http://info.internet.isi.edu:80/in-notes/rfc/files/rfc2267.txt

[2] Results of the Distributed-Systems Intruder Tools Workshop, The CERT Coordination Center, December, 1999, available at http://www.cert.org/reports/dsit_workshop.pdf

[3] The "Mac Attack," a Scheme for Blocking Internet Connections, John A. Copeland, December, 1999, available at http://www.csc.gatech.edu/~copeland. Temporary alternate URL: http://people.atl.mediaone.net/jacopeland

The CERT Coordination Center thanks Jeff Schiller of the Massachusetts Institute of Technology, Professor John Copeland and Jim Hendricks of the Georgia Institute of Technology, Jim Ellis of Sun Microsystems, Wietse Venema of IBM, Rick Forno of Network Solutions, Inc., Dave Dittrich of the University of Washington, Steve Bellovin of AT&T, Jim Duncan and John Bashinski of Cisco Systems, and MacInTouch for input and technical assistance used in the construction of this advisory.

Revision History

```
December 28, 1999: Initial release

December 28, 1999: Added information regarding a patch from Apple

March 3, 2000: Updated link to apple web page.
```