



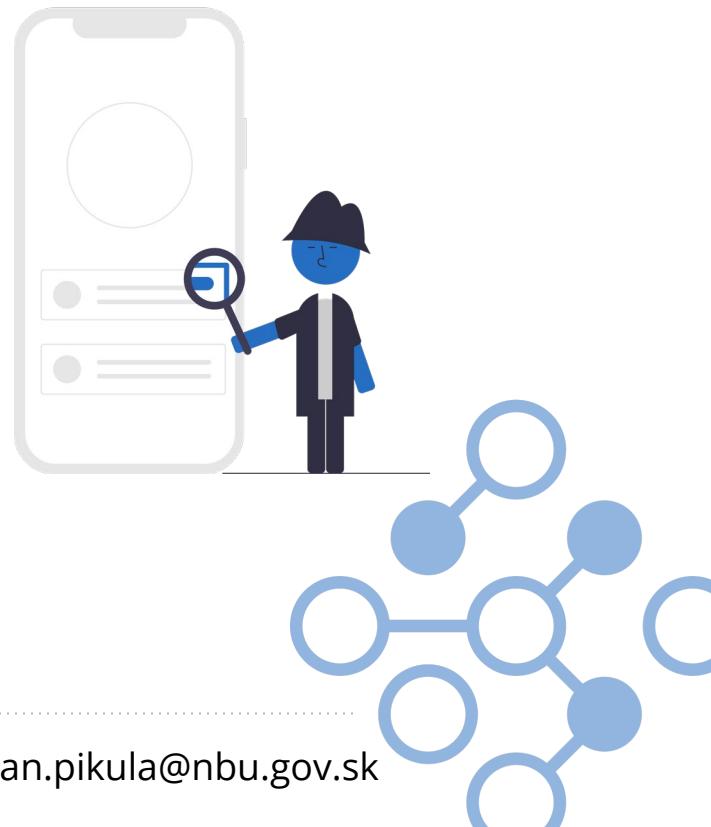
TARANIS NG

A New Tool for OSINT Analysis



OSINT is a large part of defender's routine

- **Analyze raw, unstructured OSINT data**
 - Vulnerability reports
 - Incident information
 - Threat actor TTPs and stories
 - Security news and articles
- **Discover relevant bits of information**
 - hybrid threats & disinfo narratives
- **Act on the information in a structured way**
 - Advisories
 - Reports
 - Direct action



Analysts process free-form OSINT

Hacker forums, leak sites



Slack



News sites

Social networks



E-mail



RSS, Atom feeds



TARANIS NG



github.com/SK-CERT/Taranis-NG

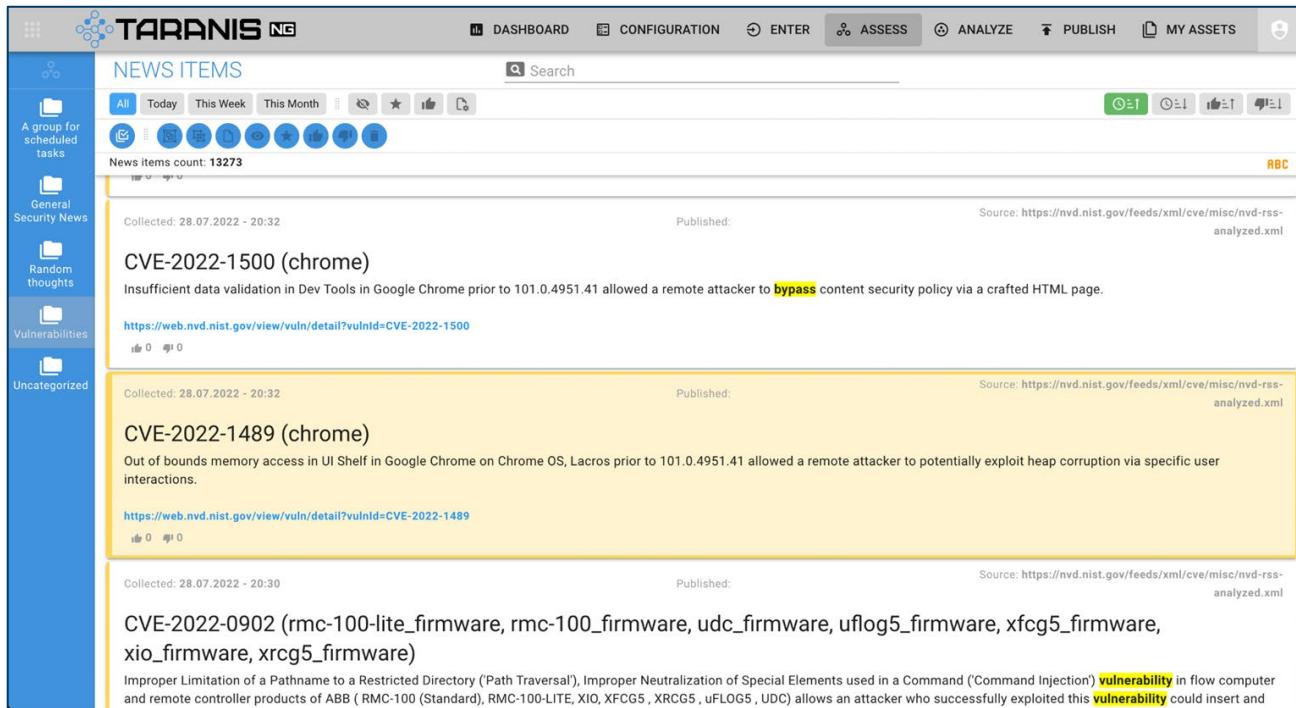


www.sk-cert.sk



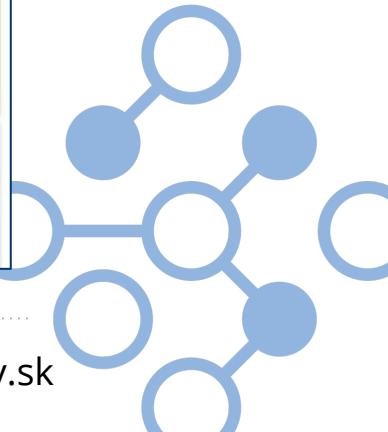
milan.pikula@nbu.gov.sk

Analysts process free-form OSINT...



The screenshot shows the Taranis NG interface with the following details:

- NEWS ITEMS** section with a count of 13273 news items.
- CVE-2022-1500 (chrome)**
Published: 28.07.2022 - 20:32
Source: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>
Description: Insufficient data validation in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to **bypass** content security policy via a crafted HTML page.
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1500>
- CVE-2022-1489 (chrome)**
Published: 28.07.2022 - 20:32
Source: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>
Description: Out of bounds memory access in UI Shelf in Google Chrome on Chrome OS, Lacros prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific user interactions.
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1489>
- CVE-2022-0902 (rmc-100-lite_firmware, rmc-100_firmware, udc_firmware, uflog5_firmware, xfcg5_firmware, xio_firmware, xrcg5_firmware)**
Published: 28.07.2022 - 20:30
Source: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>
Description: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'), Improper Neutralization of Special Elements used in a Command ('Command Injection') **vulnerability** in flow computer and remote controller products of ABB (RMC-100 (Standard), RMC-100-LITE, XIO, XFCG5 , XRCG5 , uFLOG5 , UDC) allows an attacker who successfully exploited this **vulnerability** could insert and



github.com/SK-CERT/Taranis-NG



www.sk-cert.sk



milan.pikula@nbu.gov.sk

... to create structured reports

New report item

CVSS

Value: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Base Score HIGH: 8.8 Temporal Score HIGH: 8.8 Environmental Score HIGH: 8.8

TLP

TP: CLEAR (radio button selected) TP: GREEN TP: AMBER
TP: AMBER+STRICT TP: RED

Confidentiality

UNRESTRICTED (radio button selected) CLASSIFIED CONFIDENTIAL SECRET
TOP SECRET

Description

Value: The two browsers had some random vulnerabilities spaced 12 years apart, with the same number. What a coincidence, right?

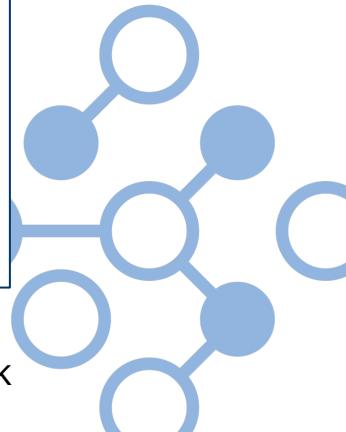
IMPORT CSV Side-by-side view Completed SAVE

Collected: 28.07.2022 - 20:32 Published: Source: https://nvd.nist.gov/feeds/xml/cve/miss/nvd-rss-analyzed.xml

CVE-2022-1489 (chrome)
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1489
0 0

Collected: 01.03.2022 - 05:23 Published: Source: https://nvd.nist.gov/feeds/xml/cve/miss/nvd-rss-analyzed.xml

CVE-2010-1489 (internet_explorer)
https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1489
0 0





github.com/SK-CERT/Taranis-NG

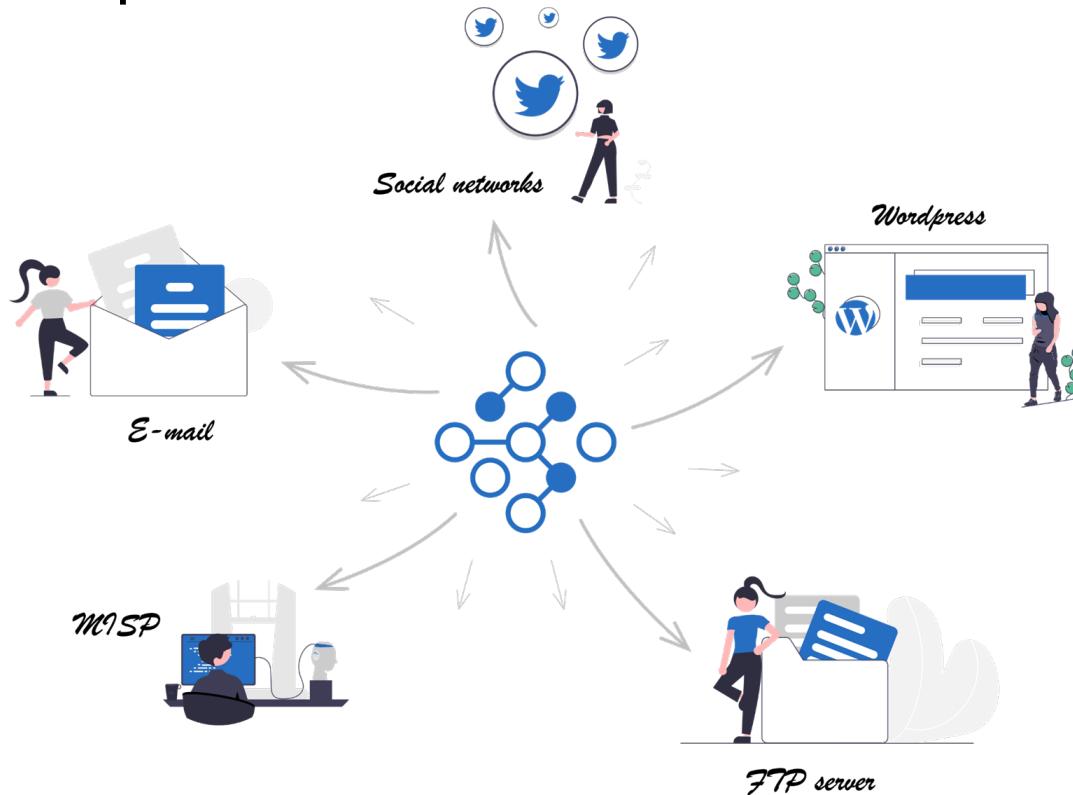


www.sk-cert.sk



milan.pikula@nbu.gov.sk

...share final products with various audiences



github.com/SK-CERT/Taranis-NG



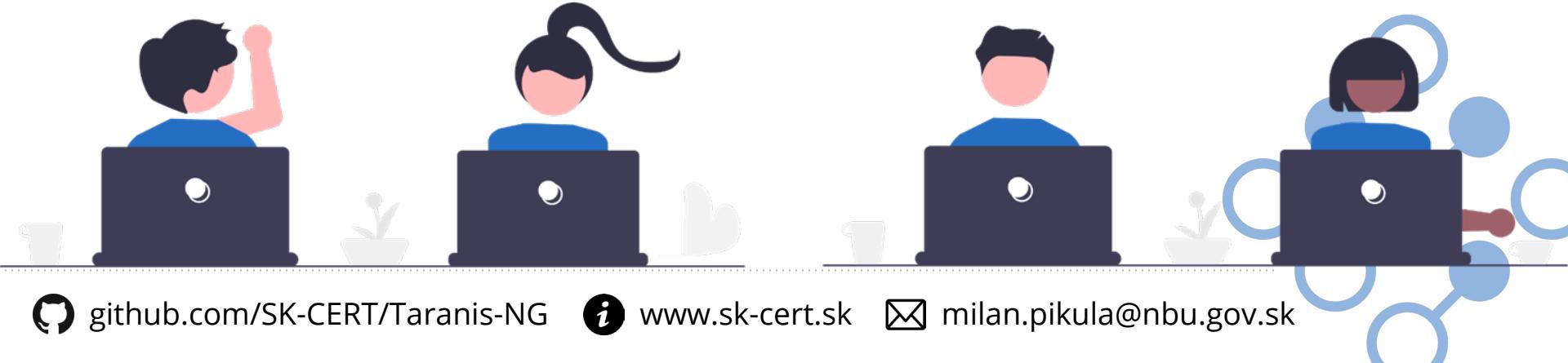
www.sk-cert.sk



milan.pikula@nbu.gov.sk

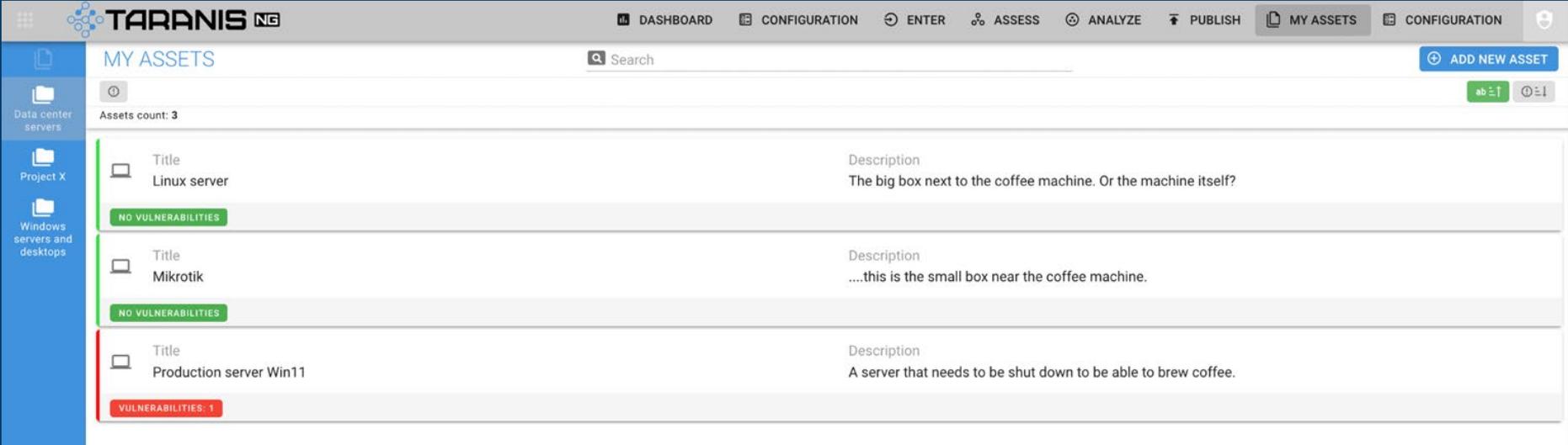
Sharing is caring - also team to team

- pinpoint information relevant to community
- watch for / on interesting news items from partner CSIRTs
- utilize distributed human intelligence



Vulnerability reports for your constituency

- self service asset management
- see vulnerabilities relevant to your technology



The screenshot shows the Taranis NG web interface. The left sidebar has icons for Data center servers, Project X, and Windows servers and desktops. The main area is titled 'MY ASSETS' and shows an 'Assets count: 3'. Each asset entry includes a title, description, and a 'NO VULNERABILITIES' or 'VULNERABILITIES: 1' button. A search bar is at the top right, and a 'MY ASSETS' button is in the top right corner.

Title	Description
Linux server	The big box next to the coffee machine. Or the machine itself?
Mikrotikthis is the small box near the coffee machine.
Production server Win11	A server that needs to be shut down to be able to brew coffee.



github.com/SK-CERT/Taranis-NG



www.sk-cert.sk



milan.pikula@nbu.gov.sk

Summary

- Target audience: CSIRTs, their constituencies, analytic centers
- End users / consumers
 - Security, System administrators
 - Any audience in need of structured reports
- Join our Slack (support, news, chat)
- Get: <https://taranis.ng/>



github.com/SK-CERT/Taranis-NG



www.sk-cert.sk



milan.pikula@nbu.gov.sk