



# TARANIS



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*



*E-mail*



*News sites*



*Social networks*



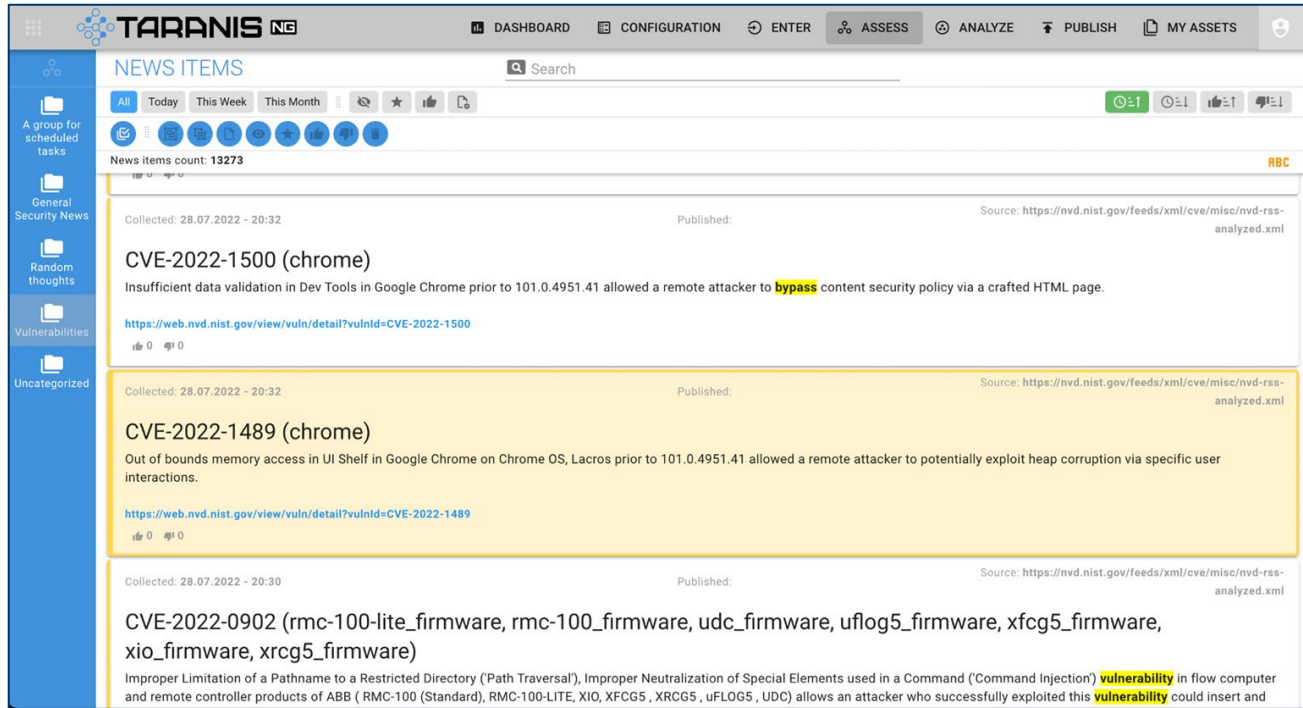
*RSS, Atom feeds*



**TARANIS NG**



# Analysts process free-form OSINT...



The screenshot displays the TARANIS NG dashboard interface. At the top, there is a navigation bar with tabs for DASHBOARD, CONFIGURATION, ENTER, ASSESS, ANALYZE, PUBLISH, and MY ASSETS. Below this, the main content area is titled 'NEWS ITEMS' and includes a search bar and filters for 'All', 'Today', 'This Week', and 'This Month'. A sidebar on the left contains navigation options: 'A group for scheduled tasks', 'General Security News', 'Random thoughts', 'Vulnerabilities', and 'Uncategorized'. The main content area shows a list of news items, each with a title, a brief description, and a source link. The items are: CVE-2022-1500 (chrome), CVE-2022-1489 (chrome), and CVE-2022-0902 (rmc-100-lite\_firmware, rmc-100\_firmware, udc\_firmware, uflog5\_firmware, xfcg5\_firmware, xio\_firmware, xrcg5\_firmware). Each item includes a 'Collected' and 'Published' timestamp, and a source link to the NVD website.

**TARANIS NG** DASHBOARD CONFIGURATION ENTER ASSESS ANALYZE PUBLISH MY ASSETS

NEWS ITEMS Search

All Today This Week This Month

News items count: 13273

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

**CVE-2022-1500 (chrome)**  
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>

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

**CVE-2022-1489 (chrome)**  
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>

Collected: 28.07.2022 - 20:30 Published: Source: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>

**CVE-2022-0902 (rmc-100-lite\_firmware, rmc-100\_firmware, udc\_firmware, uflog5\_firmware, xfcg5\_firmware, xio\_firmware, xrcg5\_firmware)**  
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



# ... to create structured reports

**CVSS**

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

Base Score HIGH 8.8

Temporal Score HIGH 8.8

Environmental Score HIGH 8.8

**TLP**

TLP-CLEAR  TLP-GREEN  TLP-AMBER  
 TLP-AMBER+STRICT  TLP-RED

**Confidentiality**

UNRESTRICTED  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?

Collected: 28.07.2022 - 20:32 Published: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>

**CVE-2022-1489 (chrome)**

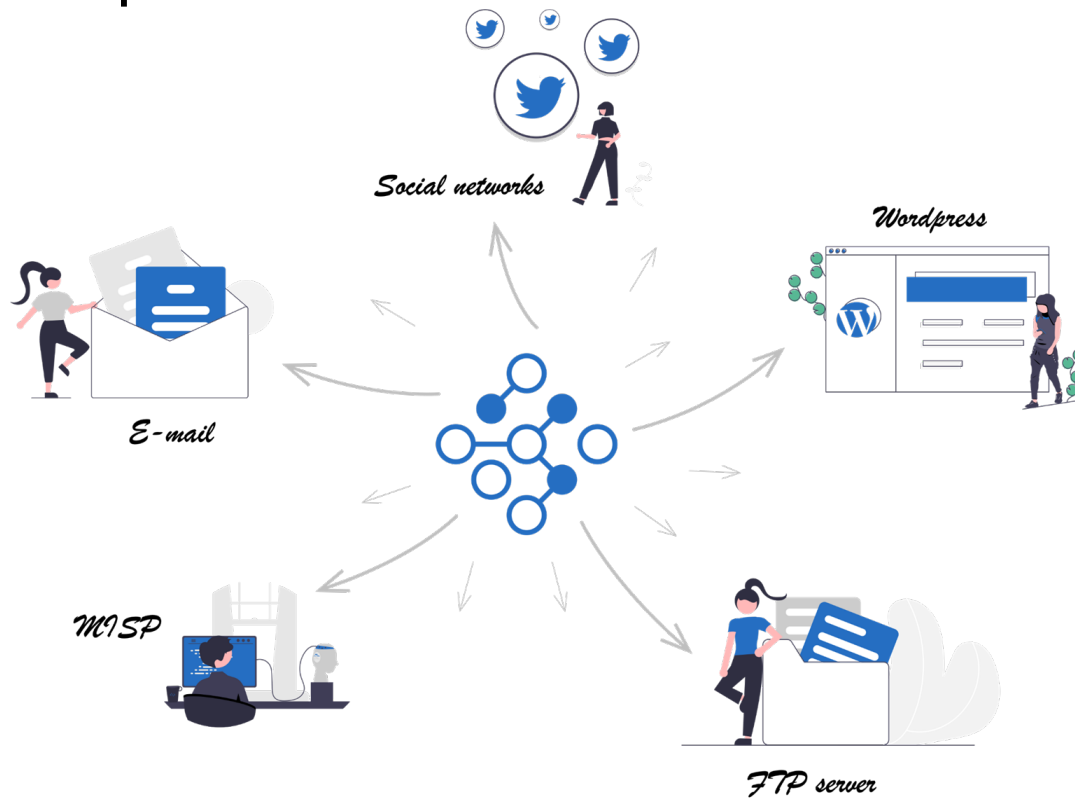
<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1489>

Collected: 01.03.2022 - 05:23 Published: <https://nvd.nist.gov/feeds/xml/cve/misc/nvd-rss-analyzed.xml>

**CVE-2010-1489 (internet\_explorer)**

<https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-1489>

# ...share final products with various audiences



# 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



[github.com/SK-CERT/Taranis-NG](https://github.com/SK-CERT/Taranis-NG)



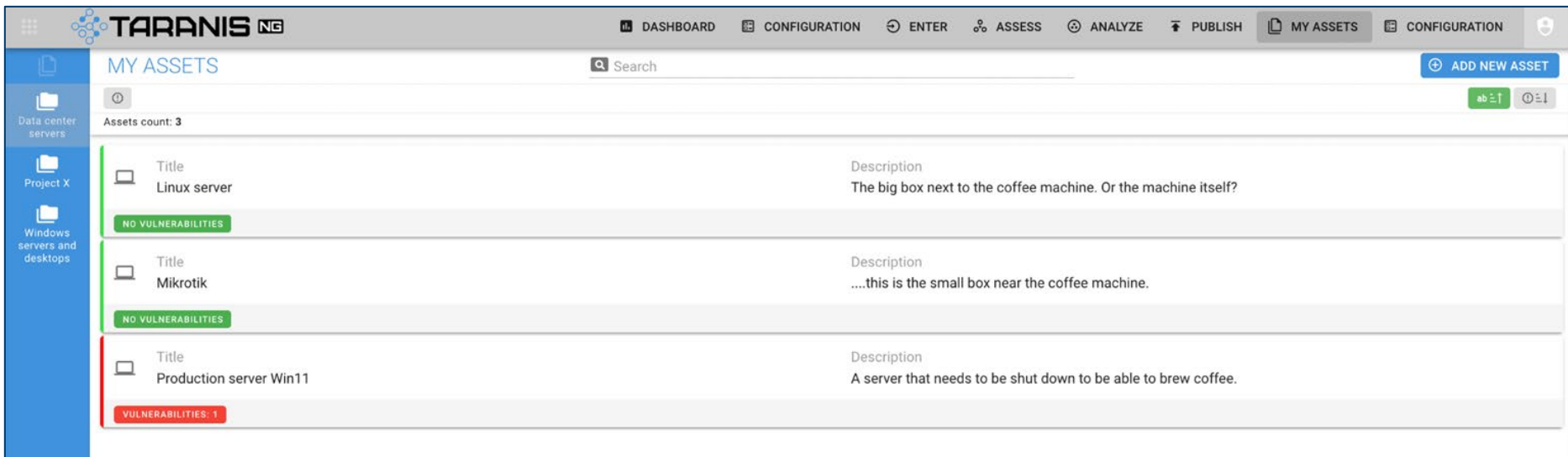
[www.sk-cert.sk](http://www.sk-cert.sk)



[milan.pikula@nbu.gov.sk](mailto:milan.pikula@nbu.gov.sk)

# Vulnerability reports for your constituency

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



The screenshot displays the Taranis NG web interface. The top navigation bar includes 'DASHBOARD', 'CONFIGURATION', 'ENTER', 'ASSESS', 'ANALYZE', 'PUBLISH', 'MY ASSETS', and 'CONFIGURATION'. The main content area is titled 'MY ASSETS' and shows a search bar and an 'ADD NEW ASSET' button. A sidebar on the left lists 'Data center servers', 'Project X', and 'Windows servers and desktops'. The main area shows a table of assets with the following details:

Title	Description	Vulnerabilities
Linux server	The big box next to the coffee machine. Or the machine itself?	NO VULNERABILITIES
Mikrotik	...this is the small box near the coffee machine.	NO VULNERABILITIES
Production server Win11	A server that needs to be shut down to be able to brew coffee.	VULNERABILITIES: 1



# 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/>

