...more than software,
your IT partner

13/03/2024

Sicurezza ICT

MILANO 28 Febbraio 2024

Are we really sure that a vulnerability with a CVSS 10 rating will cause the end of the world?

CVSS EPSS

What is CVSS?

The **Common Vulnerability Scoring System** is a standard metric in cybersecurity that quantifies the severity of vulnerabilities with a numerical score. CVSS helps prioritize responses to security threats efficiently.

Standard

IT provides a standardized method for assessing and scoring the severity of vulnerabilities from 0 to 10 across different systems and organizations

Metrics-based

It considers various factors such as exploitability, impact, and complexity to assign a numerical score to vulnerabilities.

Consistent

It allows organizations to compare and prioritize vulnerabilities to meet needs and risk management strategies

published by

FIRST
Improving Security Together

...and what about EPSS?

The **Exploit Prediction Scoring System** offers a probabilistic approach to vulnerability management. It is a data-driven model that estimates the likelihood of a software vulnerability being actively exploited in the next 30 days.

● Data-driven

It relies on historical data and daily exploitations activities to generate its predictions

● Probabilistic

It assigns scores between 0 and 1, representing the likelihood of a vulnerability being exploited

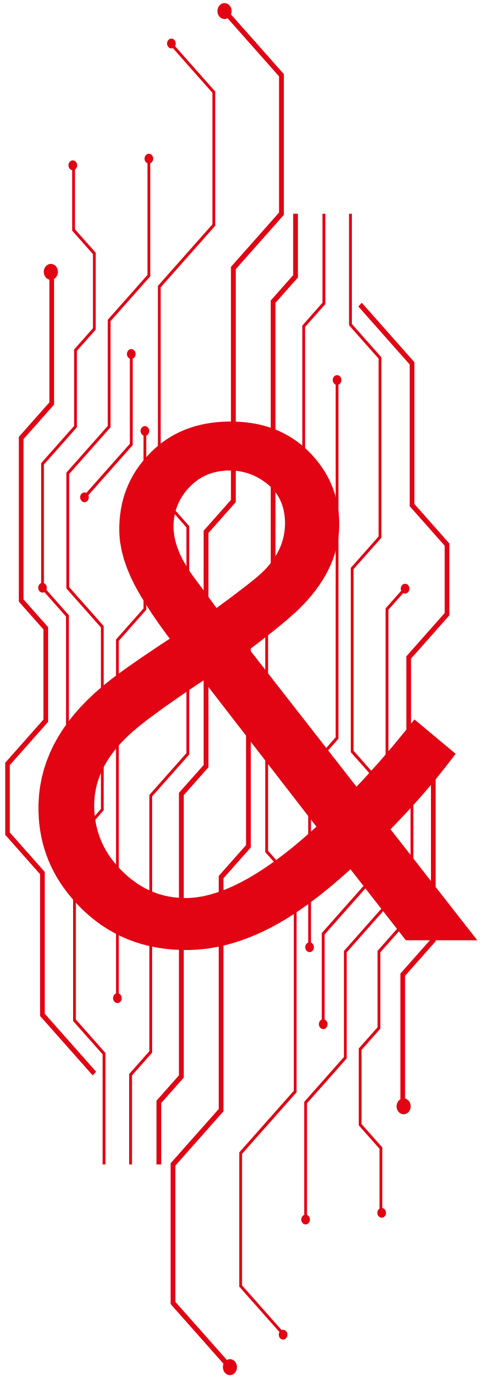
● Actionable

It helps prioritize patching efforts by highlighting vulnerabilities with a higher chance of real-world exploitation

published by

FIRST
Improving Security Together

CVSS & EPSS



Example 1

Cisco EOL Software vulnerability

CVE-2021-1459

published in April 2021

Cisco affected products:

- Firewall VPN Wireless-N RV110W
- Router VPN RV130
- Router VPN Wireless-N RV130W
- Router VPN Wireless-N RV215W

Software support ended December 2020

CVSS

9.8

EPSS

0.24%

SPOILER

It's not the end of the world!

https://www.cisco.com/c/en/us/products/collateral/routers/small-business-rv-series-routers/eos-eol-notice-c51-742771.pdf

Example 2

A new Cisco vulnerability

CVE-2023-20198

published in October 2023

CVSS
10.0

EPSS
91.92%

OMG!

Example 2

A new Cisco vulnerability

CVE-2023-20198

published in October 2023

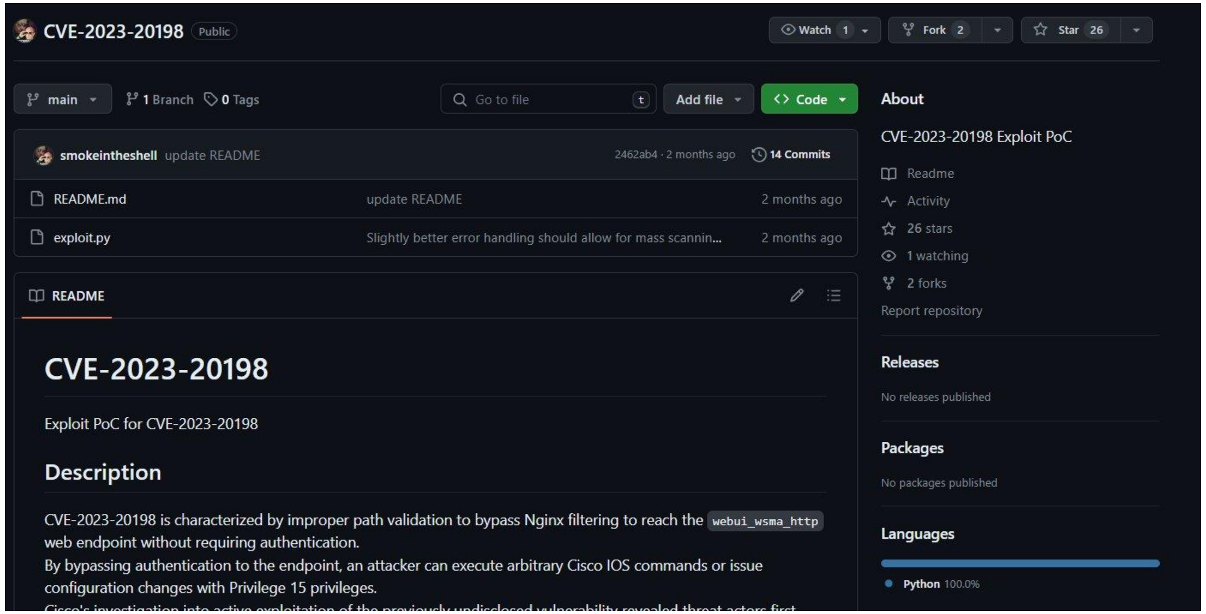
CVSS

10.0

EPSS

91.92%

OMG!



smokeintheshell update README 2462ab4 · 2 months ago

```
README.md   update README                                                2 months ago
exploit.py  Slightly better error handling should allow for mass scannin...  2 months ago
```

About

CVE-2023-20198 Exploit PoC

Readme
Activity
26 stars
1 watching
2 forks
Report repository

Releases

No releases published

Packages

No packages published

Languages

Python 100.0%

CVE-2023-20198

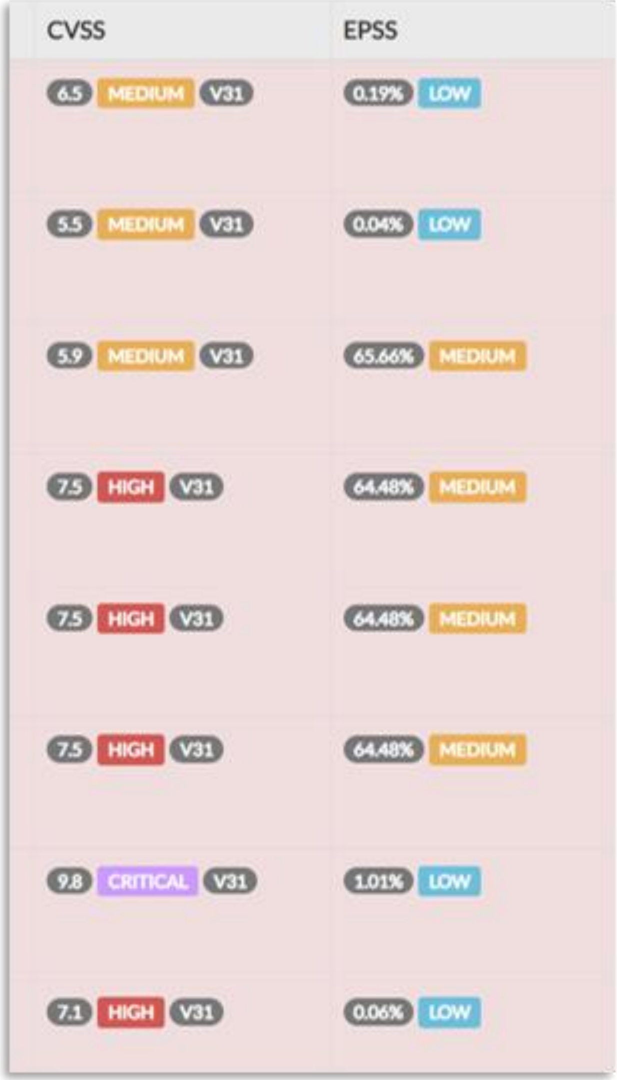
Exploit PoC for CVE-2023-20198

Description

CVE-2023-20198 is characterized by improper path validation to bypass Nginx filtering to reach the `webui_wsma_http` web endpoint without requiring authentication.
By bypassing authentication to the endpoint, an attacker can execute arbitrary Cisco IOS commands or issue configuration changes with Privilege 15 privileges.
Cisco's investigation into active exploitation of the previously undisclosed vulnerability revealed threat actors first

https://github.com/smokeintheshell/CVE-2023-20198

What to do about the future?



CVSS	EPSS
6.5 MEDIUM V31	0.19% LOW
5.5 MEDIUM V31	0.04% LOW
5.9 MEDIUM V31	65.66% MEDIUM
7.5 HIGH V31	64.48% MEDIUM
7.5 HIGH V31	64.48% MEDIUM
7.5 HIGH V31	64.48% MEDIUM
9.8 CRITICAL V31	1.01% LOW
7.1 HIGH V31	0.06% LOW

Use EPSS together with CVSS in your Threat Intelligence activities to give better insights on the detected vulnerability

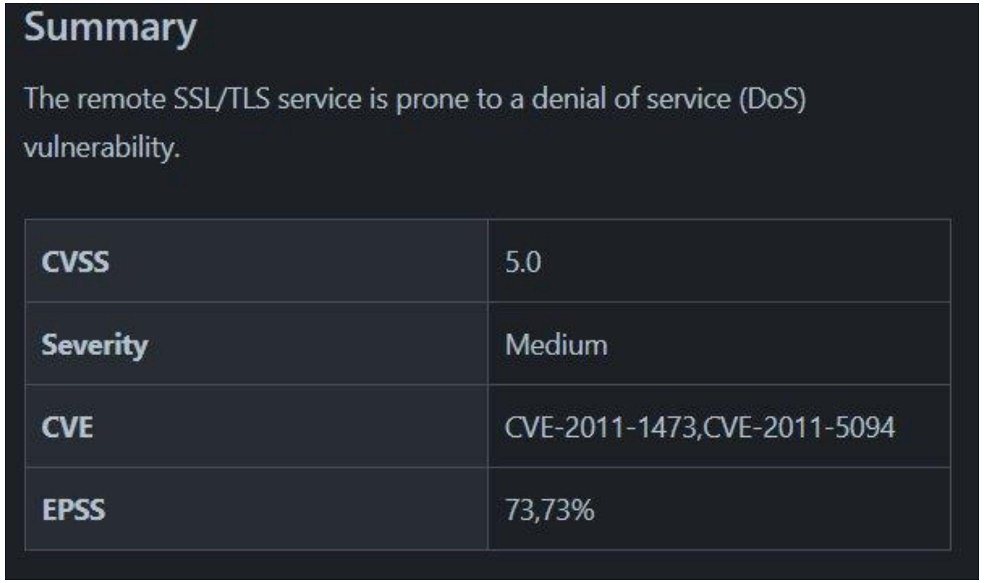
Opening ticket criteria:

- CVSS > 9.0
- CVSS > 7.0 and EPSS > 80%

Integrate EPSS in your SOC to improve your vulnerability management monthly process

Opening ticket criteria:

- CVSS > 5.0
- CVSS > 5.0 and EPSS > 60%

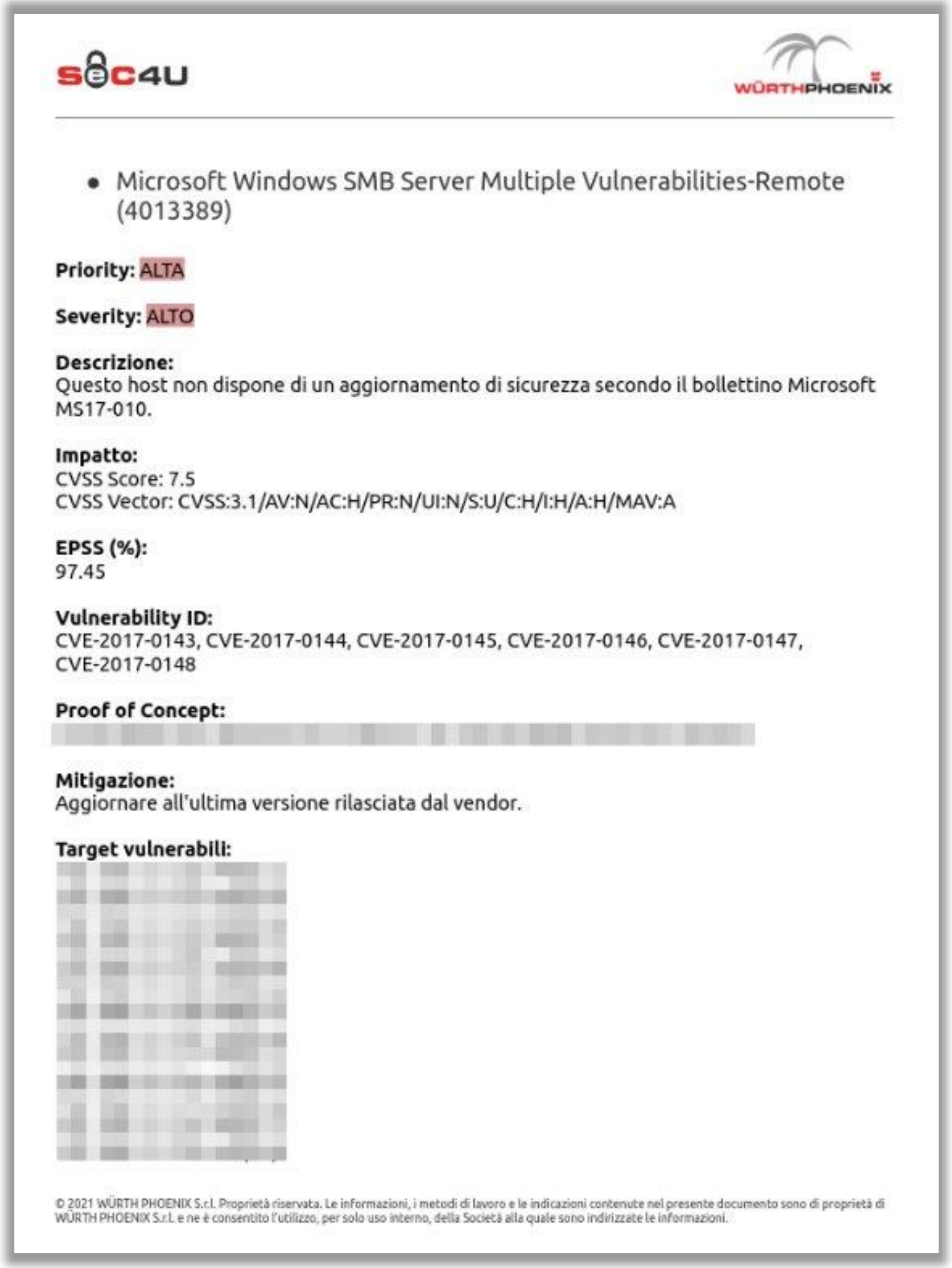


Summary

The remote SSL/TLS service is prone to a denial of service (DoS) vulnerability.

CVSS	5.0
Severity	Medium
CVE	CVE-2011-1473,CVE-2011-5094
EPSS	73,73%

Analyze EPSS in your vulnerability assessment activities



- Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Priority: ALTA

Severity: ALTO

Descrizione:
Questo host non dispone di un aggiornamento di sicurezza secondo il bollettino Microsoft MS17-010.

Impatto:
CVSS Score: 7.5
CVSS Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/MAV:A

EPSS (%):
97.45

Vulnerability ID:
CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148

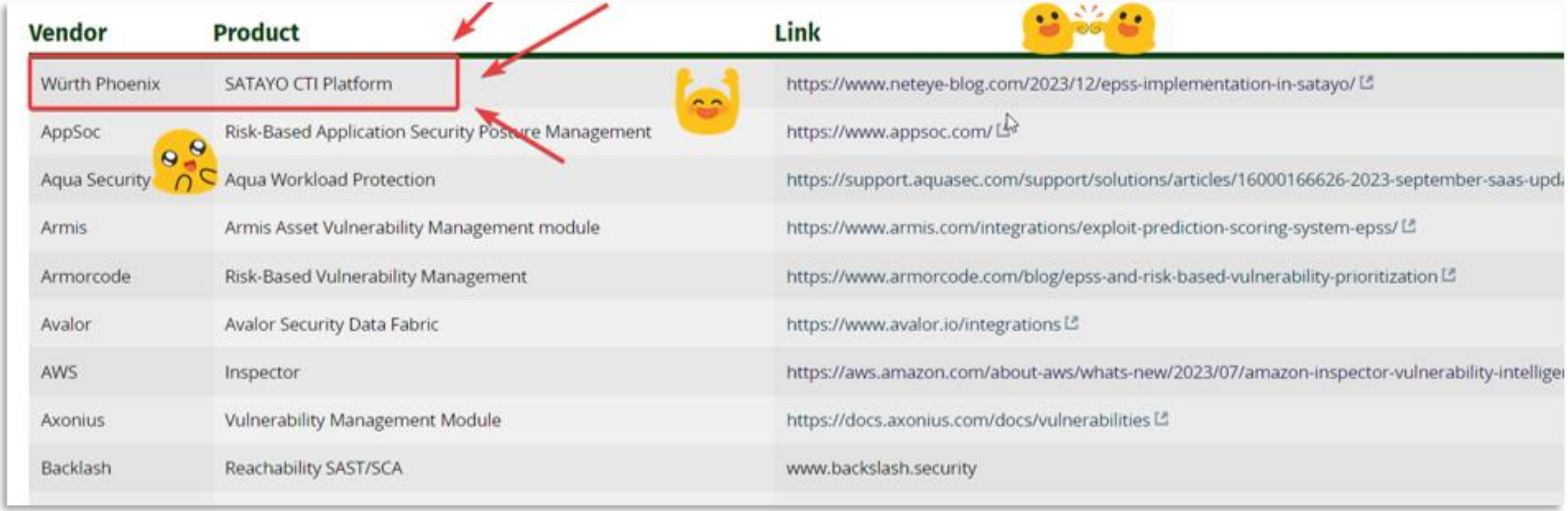
Proof of Concept:
[redacted]

Mitigazione:
Aggiornare all'ultima versione rilasciata dal vendor.

Target vulnerabili:
[redacted]

Not sure where to start?

Check FIRST's list of vendors using EPSS



Vendor	Product	Link
Würth Phoenix	SATAYO CTI Platform	https://www.neteye-blog.com/2023/12/epss-implementation-in-satayo/
AppSoc	Risk-Based Application Security Posture Management	https://www.appsoc.com/
Aqua Security	Aqua Workload Protection	https://support.aquasec.com/support/solutions/articles/16000166626-2023-september-saas-upd
Armis	Armis Asset Vulnerability Management module	https://www.armis.com/integrations/exploit-prediction-scoring-system-epss/
Armorcode	Risk-Based Vulnerability Management	https://www.armorcode.com/blog/epss-and-risk-based-vulnerability-prioritization
Avalor	Avalor Security Data Fabric	https://www.avalor.io/integrations
AWS	Inspector	https://aws.amazon.com/about-aws/whats-new/2023/07/amazon-inspector-vulnerability-intellige
Axonius	Vulnerability Management Module	https://docs.axonius.com/docs/vulnerabilities
Backlash	Reachability SAST/SCA	www.backslash.security

https://www.first.org/epss/who_is_using/

info@wuerth-phoenix.com
www.wuerth-phoenix.com

WÜRTHPHOENIX