Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Control Web Panel OS Command Injection Exploitation Increases After POC Release

Date of Publication	Admiralty Code	TA Number
January 20, 2023	A1	TA2023036

Summary

First Seen: January 2023
Affected Product: CentOS Web Panel
Impact: An unauthenticated remote code execution vulnerability in Control Web Panel (CWP) could allow attackers to run arbitrary operating system commands

CVEs

CVE	NAME	PATCH
CVE-2022-44877	CWP Control Web Panel OS Command Injection Vulnerability	✓

Vulnerability Details

On January 3, 2023, a security researcher published a proof-of-concept exploit for a vulnerability in Control Web Panel (CWP) that allows unauthenticated remote code execution. By January 6, the vulnerability was being actively exploited in the wild. The vulnerability is caused by the ability for attackers to execute bash commands when incorrect entries are logged to the system using double quotes. This allows them to remotely execute any operating system command via shell metacharacters in the login parameter (login/index.php).

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-44877	CentOS versions upto 0.9.8.1147	cpe:2.3:a:centos-webpanel:centos_web_panel:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	T1059 Command and Scripting Interpreter	TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation

Patch Details

CWP users should upgrade their versions to 0.9.8.1147 or later

References

https://viz.greynoise.io/tag/centos-web-panel-rce-cve-2022-44877-attempt?days=30

https://www.rapid7.com/blog/post/2023/01/19/etr-exploitation-of-control-web-panel-cve-2022-44877/

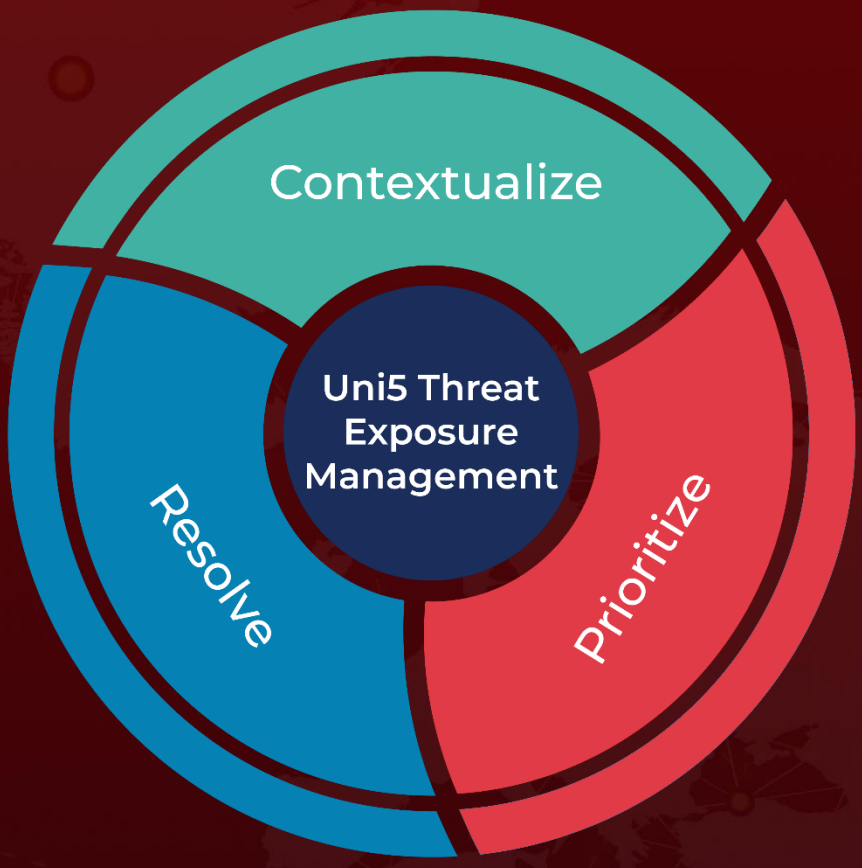
https://seclists.org/fulldisclosure/2023/Jan/1

https://www.youtube.com/watch?v=kiLfSvc1SYY

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

January 20, 2023 • 6:30 AM

More at www.hivepro.com