Hive Pro

Threat Level

Red

THREAT ADVISORY

VULNERABILITY REPORT

Linux flaws could be chained together to achieve root access

Date of Publication	Admiralty Code	TA Number
December 7, 2022	A1	TA2022286

Summary

Date: December 5, 2022
Affected Product: Linux-based environments
Impact: results in full root privileges and arbitrary code execution

CVEs

CVE	NAME	PATCH
CVE-2022-41974	Authorization bypass in Multipathd	✓
CVE-2022-41973	Symlink attack in Multipathd	✓
CVE-2022-3328	Race condition Snapd vulnerability	✓

Vulnerability Details

#1 Two vulnerabilities -CVE-2022-41974 and CVE-2022-41973 - can either be exploited individually or in combination to lead to local privilege escalation, the first potentially causing a symlink attack and the second causing an authorization bypass.

#2 Another security bug has been identified as CVE-2022-3328. It affects Snapd's Snap-confine function on Linux, which builds the Snap app execution environment.

#3 An attacker can gain full root privileges on a compromised Linux system if all three vulnerabilities are exploited successfully.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-41974	multipath-tools 0.7.0-0.9.2	cpe:2.3:a:opensvc:multipath-tools:*:*:*:*:*:*:*:*	CWE-269
CVE-2022-41973	multipath-tools 0.7.7 to 0.9.2	cpe:2.3:a:opensvc:multipath-tools:*:*:*:*:*:*:*:*	CWE-59
CVE-2022-3328	Snapd: 2.54.3 - 2.57.5	cpe:2.3:a:snapcore:snapd:*:*:*:*:*:*:*:*	CWE-362

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' & 'Patch Link' on the following pages.

Potential MITRE ATT&CK TTPs

TA0004 Privilege Escalation	T1068 Exploitation for Privilege Escalation

Patch Links

https://ubuntu.com/security/CVE-2022-3328

https://github.com/opensvc/multipath-tools/releases/tag/0.9.2

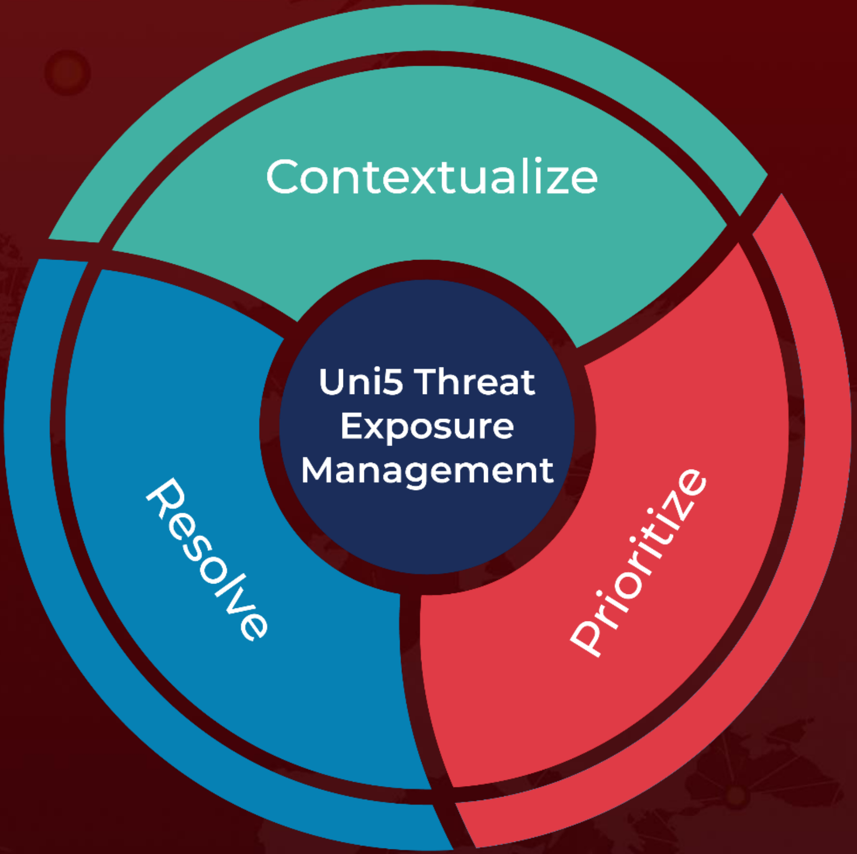
References

https://socprime.com/blog/cve-2022-41974-cve-2022-41973-cve-2022-3328-exploit-detection-three-linux-vulnerabilities-chained-to-gain-full-root-privileges/

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

December 7, 2022 • 5:00 AM

More at www.hivepro.com