Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

The Linux kernel has several security flaws

Date of Publication	Last updated date	Admiralty Code	TA Number
December 28, 2022	December 30, 2022	A1	TA2022320

Summary

First Seen: December 22, 2022
Affected Product: Linux kernel
Impact: Execute Code in the context of the Kernel

CVE

CVE	NAME	PATCH
CVE-2022-47939	Linux Kernel ksmbd Use-After-Free Remote Code Execution Vulnerability	✓
CVE-2022-47941	Linux Kernel ksmbd Memory Exhaustion Denial-of-Service Vulnerability	✓
CVE-2022-47942	Linux Kernel ksmbd Heap-based Buffer Overflow Remote Code Execution Vulnerability	✓
CVE-2022-47938	Linux Kernel ksmbd Out-Of-Bounds Read Denial-of-Service Vulnerability	✓
CVE-2022-47940	Linux Kernel ksmbd Out-Of-Bounds Read Information Disclosure Vulnerability	✓

Vulnerability Details

#1 The Linux kernel is vulnerable to a vulnerability that allows remote attackers to execute arbitrary code on affected installations. This vulnerability can be exploited without authentication, but only on systems that have ksmbd enabled. This flaw specifically affects SMB2_TREE_DISCONNECT commands. When an object's existence is not validated before operations are performed on it, the vulnerability occurs. By exploiting this vulnerability, an attacker can execute code in the kernel's context.

#2 In addition, there are several more vulnerabilities in the Linux kernel that exist due to a boundary condition and memory leak. Upon exploitation, an unauthenticated remote user can trigger an out-of-bounds read error and read the contents of memory, execute code, and cause a denial-of-service condition on the system.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-47939	Linux kernel 5.15.x before 5.15.61	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-416
CVE-2022-47941	Linux kernel: before 5.19.2	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-401
CVE-2022-47942	Linux kernel: before 5.19.2	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-122
CVE-2022-47938	Linux kernel: before 5.19.2	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-125
CVE-2022-47940	Linux kernel: before 5.18.18	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	CWE-125

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 Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**T1190** Exploit Public-Facing Application	**T1588** Obtain Capabilities
T1588.006 Vulnerabilities			

Patch Links

https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.15.61

https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.19.2

https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.18.18

References

https://www.openwall.com/lists/oss-security/2022/12/23/10

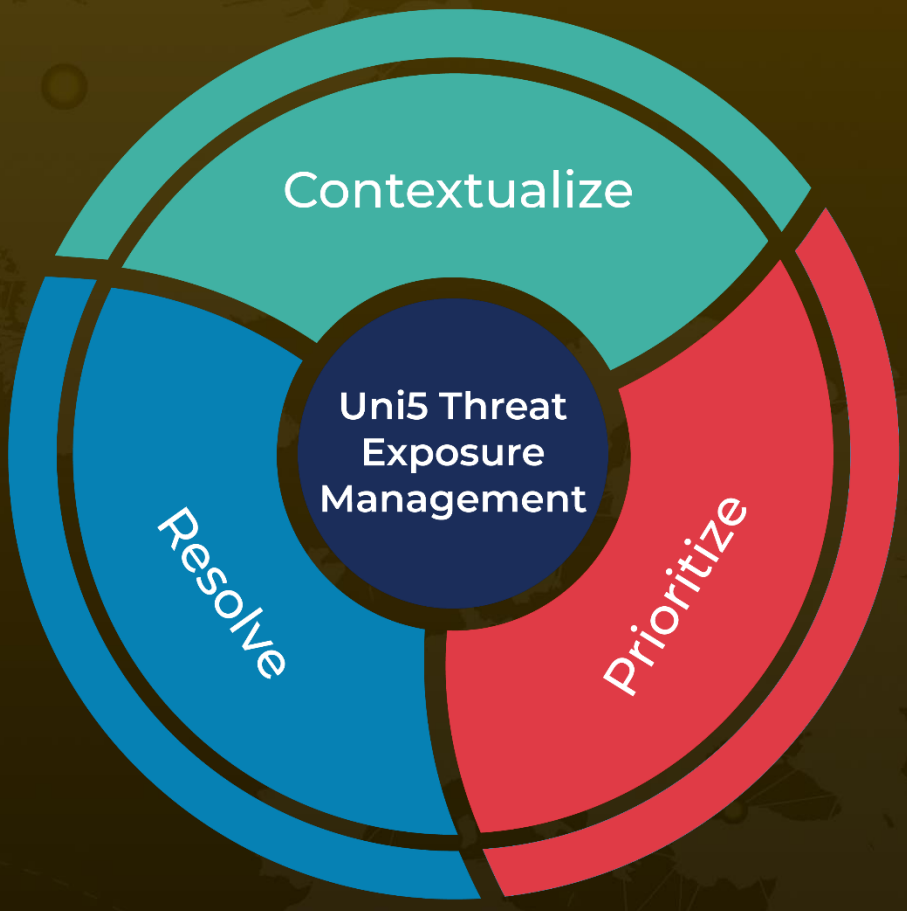
https://securityaffairs.com/140013/hacking/critical-linux-kernel-vulnerability.html

https://www.tenable.com/blog/cve-2022-47939-critical-rce-vulnerability-in-linux-kernel

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 28, 2022 • 1:00 AM

More at www.hivepro.com