Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

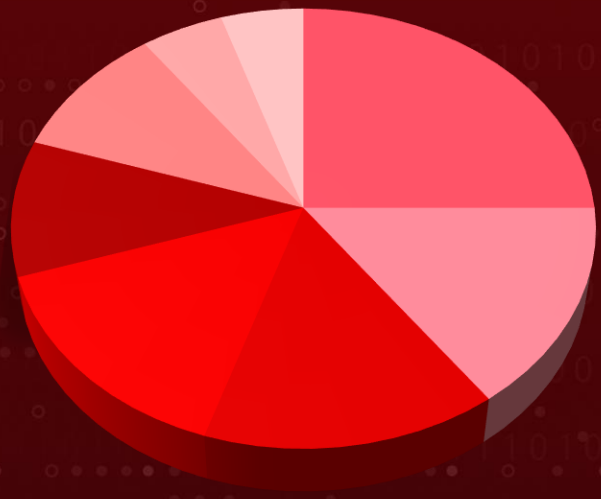
October 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
October 23, 2025	A1	TA2025323

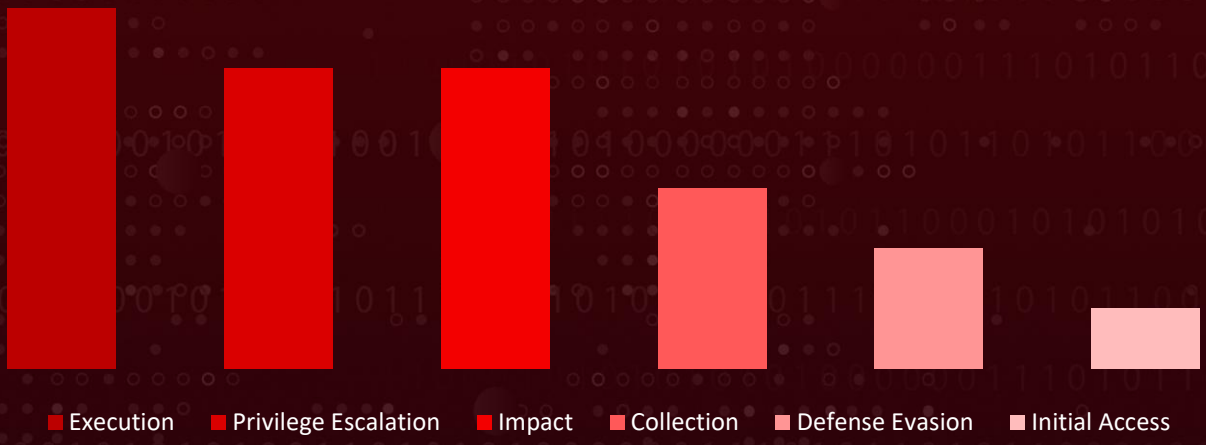
Summary

In **October**, more than **1201** new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, Red Hat, OpenSUSE, and Ubuntu. During this period, over **2169** vulnerabilities were also highlighted, with corresponding hotfixes or patches released to resolve them. These vulnerabilities span from information disclosure to privilege escalation to code execution. HiveForce Labs has identified 20 severe vulnerabilities that are exploited or have a high potential of successful exploitation, necessitating immediate attention. To ensure protection, it is essential to upgrade systems to the latest version with the necessary security patches and appropriate security controls.

Threat Distribution



Adversary Tactics



CVEs

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2021-22555*	Linux Kernel Heap Out-of-Bounds Write Vulnerability	Linux Kernel, Debian, Red Hat, Ubuntu	Privilege Escalation	Local
CVE-2023-44487*	HTTP/2 Rapid Reset Attack Vulnerability	Debian, Red Hat, Ubuntu	Denial of Service	Network
CVE-2024-23652	BuildKit Path Traversal Vulnerability	Ubuntu, SUSE, Amazon Linux	Data Destruction	Network
CVE-2024-23653	BuildKit Privilege Escalation Vulnerability	Ubuntu, Amazon Linux, SUSE	Privilege Escalation	Network
CVE-2025-21574	MySQL Server Parser Denial of Service Vulnerability	Ubuntu, Red Hat, SUSE, Debian	Denial of Service	Network
CVE-2025-38084	Linux Kernel Race Condition Vulnerability	Oracle Linux, Ubuntu, Red Hat, Debian, Amazon Linux	Memory Corruption	Local
CVE-2025-38676	Linux Kernel Stack Buffer Overflow Vulnerability	Debian, Ubuntu, Red Hat, Amazon Linux	Code Execution	Local

* Refers to **Notable CVEs**, vulnerabilities that are either exploited in zero-day attacks, included in the CISA KEV catalog, utilized in malware operations, or targeted by threat actors in their campaigns.

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-39682	Linux Kernel TLS Zero-Length Record Handling Vulnerability	SUSE, Debian, Red Hat, Ubuntu	Security Bypass	Network
CVE-2025-39866	Linux Kernel Use-After-Free Vulnerability	Debian, SUSE, Red Hat, Ubuntu	Privilege Escalation	Local
CVE-2025-39946	Linux Kernel TLS Buffer Overflow Vulnerability	Debian, Red Hat, Ubuntu, SUSE	Code Execution	Network
CVE-2025-41244*	VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability	VMware, Ubuntu, Red Hat, Debian, SUSE	Privilege Escalation	Local
CVE-2025-46817	Redis Integer Overflow in unpack()	SUSE, Red Hat, Debian	Remote Code Execution	Network
CVE-2025-46818	Redis Lua Scripting Code Injection Vulnerability	Red Hat, Debian, SUSE	Privilege Escalation	Local
CVE-2025-46819	Redis Out-of-Bounds Memory Vulnerability	Debian, Amazon Linux, SUSE	Information Disclosure	Local

* Refers to **Notable CVEs**, vulnerabilities that are either exploited in zero-day attacks, included in the CISA KEV catalog, utilized in malware operations, or targeted by threat actors in their campaigns.

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-48708	Ghostscript Argument Sanitization Vulnerability	Ubuntu, Red Hat, Debian, SUSE	Information Disclosure	Local
CVE-2025-49844*	RediShell (Redis Remote Code Execution Vulnerability)	Ubuntu, Red Hat, Debian, SUSE, Redis	Remote Code Execution	Network
CVE-2025-53547	Helm Chart Code Execution Vulnerability	SUSE, Red Hat	Code Execution	Local
CVE-2025-55315	.NET Security Feature Bypass Vulnerability	Ubuntu, Red Hat, SUSE	Security Bypass	Network
CVE-2025-6984	Langchain-community Insecure XML Parsing	Red Hat	Information Disclosure	Network
CVE-2025-55163	Netty MadeYouReset HTTP/2 DDoS Vulnerability	Red Hat, Debian	Denial of Service	Network

* Refers to **Notable CVEs**, vulnerabilities that are either exploited in zero-day attacks, included in the CISA KEV catalog, utilized in malware operations, or targeted by threat actors in their campaigns.

Notable CVEs

Notable CVEs include vulnerabilities exploited in zero-day attacks, listed in the CISA KEV catalog, used in malware operations, or targeted by threat actors in their campaigns.

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2021-22555	✗	Linux Kernel, Debian, Red Hat, Ubuntu	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:*	-
Linux Kernel Heap Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1499: Endpoint Denial of Service, T1068: Exploitation for Privilege Escalation	Linux Kernel, Debian, Red Hat, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-44487	✗	Debian, Red Hat, Ubuntu	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:*	-
HTTP/2 Rapid Reset Attack Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-400	T1588: Obtain Capabilities, T1498: Network Denial of Service, T1584: Compromise Infrastructure	Debian, Red Hat, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-41244	✗ ZERO-DAY	VMware Aria Operations and VMware Tools, Ubuntu, Red Hat, Debian, SUSE	UNC5174
	✓	**AFFECTED CPE**	**ASSOCIATED ATTACKS/RANSOMWARE**
NAME	**CISA KEV**	cpe:2.3:a:vmware:vmware_aria_operations:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:* cpe:2.3:o:suse:suse:-:*:*:*:*:*:*:*	-
VMware Aria Operations and VMware Tools Privilege Escalation Vulnerability	✗		
	CWE ID	**ASSOCIATED TTPs**	**PATCH LINKS**
	CWE-267	T1068: Exploitation for Privilege Escalation, T1036.005: Masquerading: Match Legitimate Resource Name or Location	Ubuntu, Red Hat, Debian, SUSE, VMware

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-49844	RediShell	All Versions of Redis with Lua Scripting (Before 8.2.2), Ubuntu, Red Hat, Debian, SUSE	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:redis:redis:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:-:*:*:*:*:*:*:* cpe:2.3:o:suse:suse:-:*:*:*:*:*:*:*	-
Redis Remote Code Execution Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	Ubuntu, Red Hat, Debian, SUSE, Redis

Vulnerability Details

#1

In **October**, the Linux ecosystem addressed **1201** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and code execution. Over **2169** new vulnerabilities were discovered and patched. HiveForce lab has identified **20** critical vulnerabilities that are either currently being exploited or are highly likely to be exploited in the near future.

#2

These vulnerabilities could facilitate adversarial tactics such as Execution and Privilege Escalation. Notably, four of these vulnerabilities are under active exploitation, which requires urgent attention and remediation.

#3

A long-standing vulnerability in the Linux kernel, identified as CVE-2021-22555, involves a heap out-of-bounds write flaw within the netfilter subsystem. This issue, originally disclosed as a local privilege escalation vulnerability, is now being actively exploited in real-world attacks to gain unauthorized system access. When triggered through user namespaces, it allows attackers to corrupt heap memory, elevate privileges, or cause denial-of-service (DoS) conditions.

#4

A zero-day vulnerability in the HTTP/2 protocol, tracked as CVE-2023-44487, was exploited to launch large-scale distributed denial-of-service (DDoS) attacks using a technique known as "Rapid Reset." This flaw enables remote attackers to repeatedly cancel streams at high speed, overwhelming servers and disrupting availability. This vulnerability was under active attack in August.

#5

Following this, another HTTP/2 weakness named "MadeYouReset," alongside the earlier HTTP/2 CONTINUATION Flood issue, has emerged as a potential enabler for future high-impact DoS campaigns. A VMware vulnerability, CVE-2025-41244, is currently being exploited in the wild by the threat group UNC5174 to escalate privileges from standard users to full root access within guest virtual machines.

#6

UNC5174, a China-linked actor known for its role as an initial access broker, actively leverages publicly available exploits against enterprise software to infiltrate valuable environments and facilitate follow-on compromises.

#7

Another major threat, identified as CVE-2025-49844 and referred to as "RediShell," exposes Redis servers to remote code execution. The flaw originates from a 13-year-old use-after-free bug that authenticated attackers can exploit through malicious Lua scripts. Successful exploitation allows sandbox escape and complete control over the host system, enabling credential theft, malware deployment, and lateral movement across networked systems.

#8

Separately, the website for Xubuntu, a popular open-source Linux distribution derived from Ubuntu, has been compromised. Attackers replaced legitimate torrent links with malicious ones that deliver ZIP archives containing a disguised executable. Users downloading from the affected links received malware designed to replace cryptocurrency wallet addresses with attacker-controlled ones. Although the linked wallets have not yet recorded transactions, the malware appears capable of broader functionality.

#9

In sandbox testing, the fake downloader prompted users to select a "Target Windows Version," but only listed Xubuntu options, indicating it may have been repurposed from prior Windows-targeting campaigns. The Xubuntu maintainers have since disabled downloads. This incident coincides with increased migration from Windows 10, which has reached end-of-support status, heightening the potential impact on new Linux adopters.

Recommendations

Proactive Strategies:

- Kernel Hardening and Patching: Regularly update the Linux kernel and apply all security patches immediately upon release. Utilize kernel hardening options such as grsecurity, SELinux, or AppArmor to minimize the attack surface and prevent privilege escalation.
- Network Security Controls: Implement strict network segmentation to isolate critical systems from general user environments. Use firewall policies to restrict access to network-facing services like Redis and HTTP servers. Enable rate limiting and request throttling for HTTP/2 to mitigate protocol-level abuse.
- Application Security Hygiene: Continuously monitor and patch software dependencies, particularly web servers, hypervisors, and open-source components such as Redis and VMware tools. Disable or restrict user namespaces in Linux systems where not required, as these are frequently targeted in privilege escalation exploits.
- Software Integrity Verification: Download all open-source software, including Linux distributions, exclusively from verified sources. Use checksums and GPG signatures to validate file integrity before installation. Implement internal mirrors or repositories to reduce exposure to supply chain compromises.
- Secure Configuration of Virtualized Environments: Harden virtualization platforms by isolating management interfaces, disabling unnecessary services, and regularly auditing guest VM permissions.

Reactive Strategies:

- Memory and Process Inspection: Perform immediate memory capture and live process analysis on compromised systems to identify heap corruption, rogue Lua scripts, or unauthorized kernel modules. Use forensic tools to trace privilege escalation or code execution attempts related to the identified CVEs. Preserve evidence before initiating cleanup to support post-incident analysis.
- Service Restoration from Trusted Baselines: Rebuild affected servers, Redis instances, or hypervisors from verified, uncompromised images. Reapply hardened configurations, validate patch levels, and restore critical data only from integrity-verified backups. Conduct a configuration drift analysis before reintroducing systems to production.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2021-22555*	T1499: Endpoint Denial of Service, T1068: Exploitation for Privilege Escalation	DS0015: Application Log Content, DS0029: Network Traffic Content, DS0009: Process Creation	M1037: Filter Network Traffic, M1048: Application Isolation and Sandboxing	Linux Kernel, Debian, Red Hat, Ubuntu
CVE-2023-44487*	T1588: Obtain Capabilities, T1498: Network Denial of Service, T1584: Compromise Infrastructure	DS0029: Network Traffic Content, DS0035: Response Metadata, DS0038: Passive DNS	M1037: Filter Network Traffic	Debian, Red Hat, Ubuntu
CVE-2024-23652	T1203: Exploitation for Client Execution	DS0022: File Modification, DS0015: Application Log Content	M1048: Application Isolation and Sandboxing, M1051: Update Software	Ubuntu, SUSE, Amazon Linux
CVE-2024-23653	T1068: Exploitation for Privilege Escalation	DS0009: Process Creation	M1048: Application Isolation and Sandboxing	Ubuntu, Amazon Linux, SUSE
CVE-2025-21574	T1499: Endpoint Denial of Service	DS0015: Application Log Content, DS0029: Network Traffic Content	M1037: Filter Network Traffic	Ubuntu, Red Hat, SUSE, Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-38084	T1068: Exploitation for Privilege Escalation, T1485: Data Destruction	DS0009: Process Creation, DS0022: File Modification	M1048: Application Isolation and Sandboxing, M1053: Data Backup, M1018: User Account Management	✓ Oracle Linux, Ubuntu, Red Hat, Debian, Amazon Linux
CVE-2025-38676	T1059: Command and Scripting Interpreter	DS0009: Process Creation, DS0012: Script Execution, DS0017: Command Execution	M1038: Execution Prevention, M1026: Privileged Account Management, M1033: Limit Software Installation	✓ Debian, Ubuntu, Amazon Linux ✗ Red Hat
CVE-2025-39682	T1211: Exploitation for Defense Evasion	DS0015: Application Log Content, DS0009: Process Creation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1051: Update Software	✓ SUSE, Debian, Red Hat, Ubuntu
CVE-2025-39866	T1068: Exploitation for Privilege Escalation	DS0009: Process Creation	M1048: Application Isolation and Sandboxing	✓ Debian ✗ SUSE, Red Hat, Ubuntu
CVE-2025-39946	T1059: Command and Scripting Interpreter	DS0009: Process Creation, DS0012: Script Execution, DS0017: Command Execution	M1038: Execution Prevention, M1026: Privileged Account Management, M1033: Limit Software Installation	✓ Debian ✗ Red Hat, Ubuntu, SUSE
CVE-2025-41244*	T1068: Exploitation for Privilege Escalation, T1036.005: Masquerading: Match Legitimate Resource Name or Location	DS0009: Process Creation, DS0017: Command Execution, DS0022: File Metadata, DS0019: Service Metadata	M1048: Application Isolation and Sandboxing, M1045: Code Signing, M1022: Restrict File and Directory Permissions	✓ Ubuntu, Red Hat, Debian, SUSE, VMware

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-46817	T1068: Exploitation for Privilege Escalation, T1036.005: Masquerading: Match Legitimate Resource Name or Location	DS0009: Process Creation, DS0017: Command Execution, DS0022: File Metadata, DS0019: Service Metadata	M1048: Application Isolation and Sandboxing, M1045: Code Signing, M1022: Restrict File and Directory Permissions	✓ SUSE, Red Hat, Debian
CVE-2025-46818	T1068: Exploitation for Privilege Escalation, T1036.005: Masquerading: Match Legitimate Resource Name or Location	DS0009: Process Creation, DS0017: Command Execution, DS0022: File Metadata, DS0019: Service Metadata	M1048: Application Isolation and Sandboxing, M1045: Code Signing, M1022: Restrict File and Directory Permissions	✓ Debian, SUSE ✗ Red Hat
CVE-2025-46819	T1005: Data from Local System	DS0017: Command Execution	M1057: Data Loss Prevention	✓ Debian, Amazon Linux, SUSE
CVE-2025-48708	T1005: Data from Local System	DS0017: Command Execution	M1057: Data Loss Prevention	✓ Ubuntu, Debian, SUSE ✗ Red Hat
CVE-2025-49844*	T1059: Command and Scripting Interpreter, T1497: Virtualization/Sandbox Evasion	DS0009: Process Creation, DS0012: Script Execution, DS0017: Command Execution	M1038: Execution Prevention, M1026: Privileged Account Management, M1033: Limit Software Installation, M1040: Behavior Prevention on Endpoint	✓ Ubuntu, Red Hat, Debian, SUSE, Redis

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-53547	T1059: Command and Scripting Interpreter	DS0009: Process Creation, DS0012: Script Execution, DS0017: Command Execution	M1038: Execution Prevention, M1026: Privileged Account Management, M1033: Limit Software Installation	SUSE, Red Hat
CVE-2025-55315	T1211: Exploitation for Defense Evasion	DS0015: Application Log Content, DS0009: Process Creation	M1048: Application Isolation and Sandboxing, M1050: Exploit Protection, M1051: Update Software	Ubuntu, Red Hat, SUSE
CVE-2025-6984	T1005: Data from Local System	DS0017: Command Execution	M1057: Data Loss Prevention	Red Hat
CVE-2025-55163	T1496: Resource Hijacking	DS0015: Application Log Content, DS0017: Command Execution, DS0029: Network Traffic Flow	-	Red Hat, Debian

References

https://lore.kernel.org/linux-cve-announce/

https://github.com/leonov-av/linux-patch-wednesday

https://www.debian.org/security/#DSAS

https://lists.ubuntu.com/archives/ubuntu-security-announce/

https://access.redhat.com/security/security-updates/

https://lists.opensuse.org/archives/list/security-announce@lists.opensuse.org/

https://hivepro.com/threat-advisory/http-2-zero-day-exploited-for-the-most-explosive-ddos-attacks/

https://hivepro.com/threat-advisory/leaky-vessels-in-cloud-environments-shake-docker-and-beyond/

https://hivepro.com/threat-advisory/vmware-aria-and-tools-vulnerabilities-fixed-amid-ongoing-exploitation/

https://hivepro.com/threat-advisory/redis-under-siege-redishell-flaw-opens-door-to-remote-code-execution/

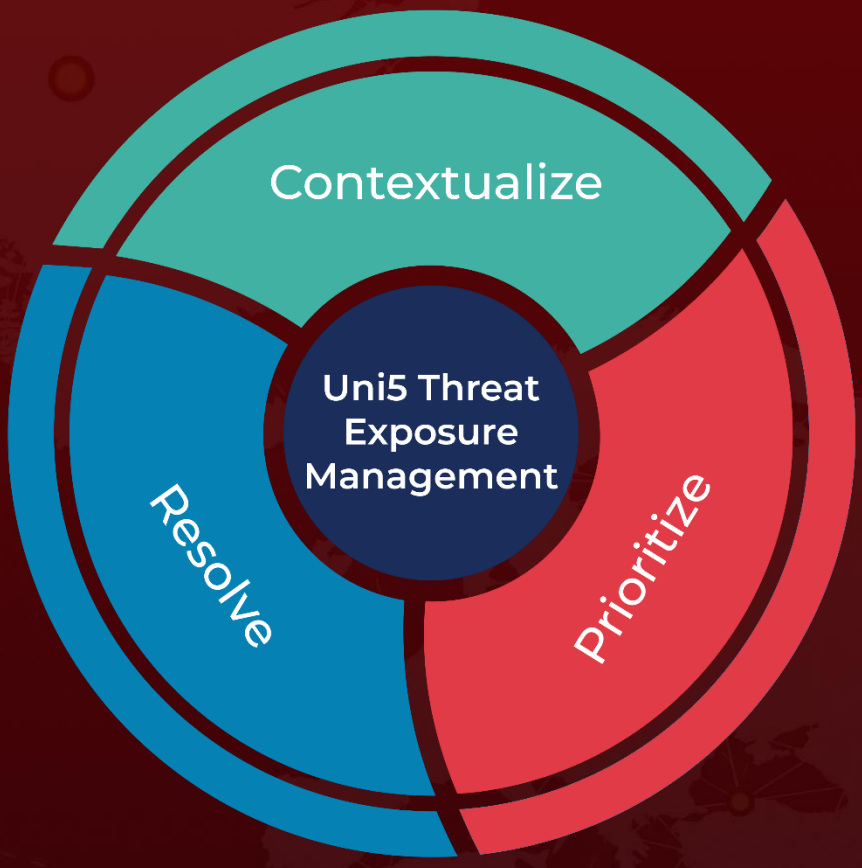
https://deepness-lab.org/publications/madeyoureset/

https://blog.qualys.com/vulnerabilities-threat-research/2023/10/10/cve-2023-44487-http-2-rapid-reset-attack

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

October 23, 2025 . 3:30 PM

More at www.hivepro.com