

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

August 2025 Linux Patch Roundup

Date of Publication

August 27, 2025

Admiralty Code

A1

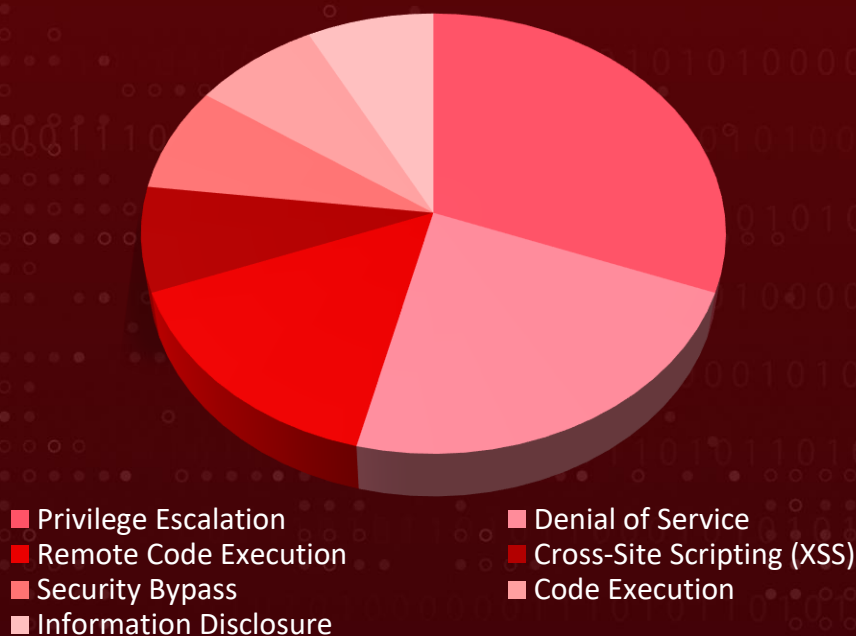
TA Number

TA2025260

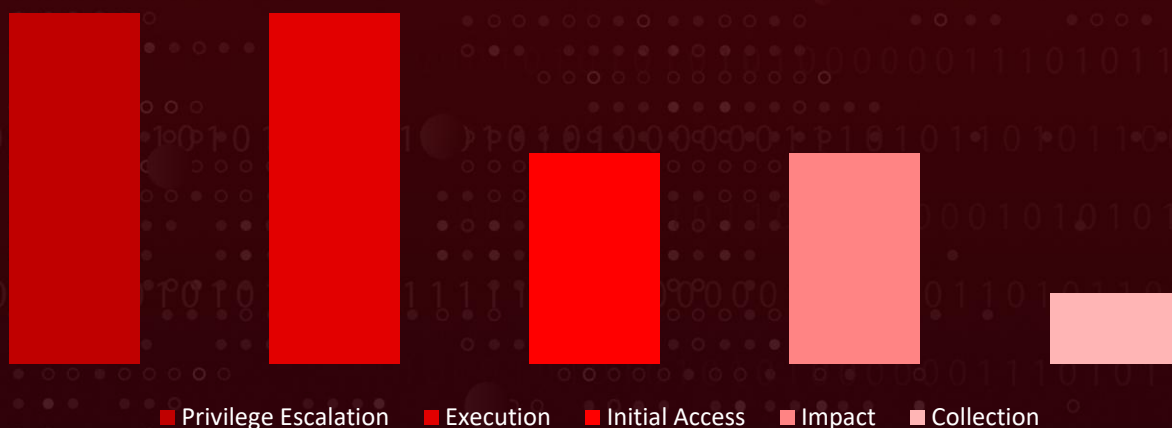
Summary

In August, more than **1305** 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 **1908** 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 **13 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-2019-11135*	ZombieLoad v2 (Intel Processors Information Disclosure Vulnerability)	Intel, Debian, Ubuntu, Red Hat	Information Disclosure	Local
CVE-2020-11022*	jQuery Cross-Site Scripting (XSS) Vulnerability	jQuery, Oracle Linux, Ubuntu, Red Hat, Debian	Cross-Site Scripting (XSS)	Network
<u>CVE-2022-2586*</u>	Linux Kernel Use-After-Free Vulnerability	Linux Kernel, Ubuntu, Red Hat, Debian	Privilege Escalation	Local
CVE-2025-23266*	NVIDIAScape (NVIDIA Container Toolkit Privilege Escalation Vulnerability)	Nvidia, Red Hat, Amazon Linux	Privilege Escalation and Account Takeover	Social engineering
CVE-2025-46811	SUSE Manager Remote Code Execution Vulnerability	SLES15-SP4-Manager-Server-4-3-BYOS SUSE Manager Server	Remote Code Execution	Remote, network-based
CVE-2025-48976	Apache Commons FileUpload Denial of Service (DoS) Vulnerability	Apache, Red Hat, Debian, Ubuntu	Denial of Service	Network
CVE-2025-49125	Apache Tomcat Authentication Bypass Vulnerability	Apache, Debian, Red Hat, Ubuntu	Unauthorized Access	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.




CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-54424	fit2cloud 1Panel Remote Code Execution Vulnerability	1Panel, SUSE	Remote Code Execution	Network
CVE-2025-6018	Linux Pluggable Authentication Modules Local Privilege Escalation (LPE) vulnerability	SUSE, Debian	Privilege Escalation	Local
CVE-2025-7425	GNOME libxslt Use-After-Free Vulnerability	Red Hat, SUSE, Debian	Memory Corruption	Local
CVE-2025-6000	Hashicorp Vault Arbitrary Code Execution Vulnerability	HashiCorp, SUSE	Code Execution	Network
CVE-2025-5999	HashiCorp Vault Privilege Escalation Vulnerability	HashiCorp, SUSE, Red Hat	Privilege Escalation	Network
CVE-2025-49796	GNOME libxml2 Out-of-Bounds Read Memory Corruption Vulnerability	Red Hat, Debian, Rocky Linux, Ubuntu, Amazon Linux	Memory Corruption	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-2019-11135	ZombieLoad v2	Intel, Debian, Ubuntu, Red Hat	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:intel:core_firmware:~:*~:*~:*~:*~* cpe:2.3:o:debian:debian_linux:~:*~:*~:*~:*~* cpe:2.3:o:canonical:ubuntu_linux:~:*~:*~:*~:*~* cpe:2.3:o:redhat:enterprise_linux:~:*~:*~:*~:*~*	-
ZombieLoad v2 (Intel Processors Information Disclosure Vulnerability)			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-399	T1056: Input Capture, T1005: Data from Local System	Intel , Debian , Ubuntu , Red Hat

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-11022		jQuery, Oracle Linux, Ubuntu, Red Hat, Debian	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:* cpe:2.3:a:oracle:weblogic_server:*:*:*:*:*:* cpe:2.3:a:redhat:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*	-
jQuery Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1203: Exploitation for Client Execution, T1059.007: JavaScript	jQuery , Ubuntu , Oracle Linux , Red Hat , Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2022-2586		Linux Kernel, Ubuntu, Red Hat, Debian	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOM WARE
NAME	CISA KEY	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*	-
Linux Kernel Use-After-Free Vulnerability		cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:* cpe:2.3:a:redhat:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*	
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-416	T1068:Exploitation for Privilege Escalation, T1499: Endpoint Denial of Service	Linux Kernel , Ubuntu , Red Hat , Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-23266	NVIDIAScape	Nvidia, Red Hat, Amazon Linux	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:nvidia:*:*:*:*:*:*:* cpe:2.3:a:redhat:*:*:*:*:*:*:* cpe:2.3:o:alma:linux:*:*:*:*:*:*:*	-
NVIDIAScape (NVIDIA Container Toolkit Privilege Escalation Vulnerability)		ASSOCIATED TTPs	PATCH LINKS
	CWE ID		
	CWE-426	T1204.003: Malicious Image, T1610: Deploy Container, T1574.006: Dynamic Linker Hijacking, T1068: Exploitation for Privilege Escalation	Nvidia , Red Hat , Amazon Linux

Vulnerability Details

#1

In August, the Linux ecosystem addressed over **1900** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and code execution. Over **1305** new vulnerabilities were discovered and patched. HiveForce lab has identified 13 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 Initial Access, Execution, and Privilege Escalation. Notably, four of these vulnerabilities are under active exploitation, which requires urgent attention and remediation.

#3

A vulnerability known as ZombieLoad v2 (CVE-2019-11135) affects certain Intel processors through the TSX Asynchronous Abort (TAA) mechanism. This flaw allows local, authenticated users to exploit speculative execution and leak sensitive data. Debian's security tracker notes that the Jessie release of the Xen hypervisor remains "unfixed" due to its end-of-life (EOL) status.

#4

Since EOL software no longer receives patches, running Xen on Jessie leaves systems permanently exposed to attacks like TAA, making them particularly high-risk in modern environments. Migrating to supported Xen versions on maintained Debian releases is therefore essential. These versions receive regular patches and community support, ensuring protection against exploits such as CVE-2019-11135 while maintaining system stability and compliance.

#5

A related vulnerability, [CVE-2019-19338](#), stems from an incomplete fix for ZombieLoad v2 within the Linux kernel. It specifically impacts guests running on Cascade Lake Intel CPUs when Transactional Synchronization Extensions (TSX) are enabled.

#6

The flaw occurs because guests fail to properly clear architectural buffers using the VERW instruction, creating opportunities for sensitive data leakage. This presents a serious confidentiality risk in virtualized environments. Mitigations include applying kernel patches or disabling TSX on the host, both of which have been implemented in later Linux kernel updates and supported distributions such as Red Hat Enterprise Linux 7 and 8.



#7

Another critical flaw, **NVIDIAScape (CVE-2025-23266)**, was found in the NVIDIA Container Toolkit. The vulnerability lies in how the toolkit handles the Open Container Initiative (OCI) hook "createContainer." Misconfiguration here allows attackers to execute arbitrary code with elevated privileges, enabling privilege escalation, data tampering, denial-of-service attacks, and even container escape. A successful exploit could lead to complete server compromise, posing a severe threat to AI cloud environments that rely heavily on GPU containers.

#8

CVE-2025-54424 affects 1Panel, a management interface and MCP server for Linux environments. The flaw allows attackers to compromise backend services used for managing websites, containers, databases, files, and large language model (LLM) tasks. The ease of exploitation depends on server exposure and configuration, but successful exploitation can lead to full compromise of LLM management functions.

#9

Two additional vulnerabilities, CVE-2025-6018 and **CVE-2025-6019**, can be chained together to achieve root access on most Linux distributions. CVE-2025-6018 involves the Pluggable Authentication Modules (PAM) configuration in openSUSE Leap 15 and SUSE Linux Enterprise 15, allowing unprivileged local attackers a path to escalation. When combined with CVE-2025-6019, attackers can reliably gain full root privileges. With root access, adversaries could disable endpoint defenses, implant persistent backdoors, or modify configurations, severely undermining system security.

Recommendations

Proactive Strategies:



Decommission End-of-Life Software: Avoid running unsupported or EOL platforms such as Debian Jessie with Xen, as they no longer receive critical fixes. Migrating to actively maintained versions reduces long-term exposure to unresolved security flaws.



Hardened Configurations: Apply strict configuration baselines for container runtimes, PAM modules, and management platforms. For example, disabling TSX on Intel hosts, restricting OCI hook usage in container toolkits, and securing SUSE Manager authentication pathways help limit attack surfaces.



Principle of Least Privilege: Restrict operator permissions and enforce granular access controls within Vault, 1Panel, and other privileged management systems. Preventing excessive token rights and ensuring proper segmentation can minimize escalation risks like CVE-2025-5999 and CVE-2025-54424.



Harden Server Configurations: Apply server hardening best practices by disabling unnecessary services, enforcing least privilege file system permissions, and securing sensitive directories. Implement strict authentication protocols and avoid insecure defaults, such as unrestricted file uploads. Validate all file uploads with type, size, and metadata checks, and regularly audit configurations against recognized security baselines.



Security Monitoring and Logging: Enable robust logging for privilege changes, token escalations, and abnormal container or process executions. Monitoring multipart upload requests, PAM activity, and XML parsing behavior can provide early detection of exploitation attempts.

Reactive Strategies:



System Isolation and Containment: Immediately isolate affected workloads, containers, or management servers to prevent further spread. In cloud environments, quarantine compromised nodes and restrict API interactions until integrity is restored.












Deploy Network Traffic Analysis for Unusual Patterns: Continuously monitor inbound and outbound network traffic to detect anomalies such as unexpected SSH connections, unusual data flows, or communication over non-standard ports. Establish behavioral baselines for normal traffic and configure alerts for deviations, as these may indicate exploitation attempts targeting vulnerabilities. Integrating NTA with SIEM/EDR platforms enhances real-time detection and rapid response.




Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2019-11135	T1056: Input Capture, T1005: Data from Local System	DS0009: Process Creation	M1057: Data Loss Prevention	 Intel, Debian, Ubuntu, Red Hat
CVE-2020-11022	T1203: Exploitation for Client Execution, T1059.007: JavaScript	DS0017: Command Execution	M1051: Update Software, M1050: Exploit Protection	 jQuery, Ubuntu, Oracle Linux, Red Hat, Debian
CVE-2022-2586	T1068: Exploitation for Privilege Escalation, T1499: Endpoint Denial of Service	DS0029: Network Traffic, DS0009: Process Creation	M1037: Filter Network Traffic, M1051: Update Software	 Linux Kernel, Ubuntu, Red Hat, Debian
CVE-2025-23266	T1204.003: Malicious Image, T1610: Deploy Container, T1574.006: Dynamic Linker Hijacking, T1068: Exploitation for Privilege Escalation	DS0015: Application Log Content, DS0032: Container Creation	M1047: Audit, M1030: Network Segmentation, M1018: User Account Management, M1051: Update Software	 Nvidia, Red Hat, Amazon Linux
CVE-2025-46811	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	DS0029: Network Traffic, DS0015: Application Log, DS0017: Command Execution	M1030: Network Segmentation, M1026: Privileged Account Management	 SUSE



CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-48976	T1499: Endpoint Denial of Service	<u>DS0015: Application Log</u> , <u>DS0029: Network Traffic Flow</u>	<u>M1037: Filter Network Traffic</u>	<div>  <u>Apache, Red Hat, Debian</u> </div> <div>  <u>Ubuntu</u> </div>
CVE-2025-49125	T1190: Exploit Public-Facing Application	<u>DS0015: Application Log Content</u> , <u>DS0029: Network Traffic</u>	<u>M1035: Limit Access to Resource Over Network</u> , <u>M1030: Network Segmentation</u> , <u>M1026: Privileged Account Management</u>	<div>  <u>Apache, Debian, Red Hat</u> </div> <div>  <u>Ubuntu</u> </div>
CVE-2025-54424	T1190: Exploit Public-Facing Application	<u>DS0015: Application Log Content</u> , <u>DS0029: Network Traffic</u>	<u>M1035: Limit Access to Resource Over Network</u> , <u>M1030: Network Segmentation</u> , <u>M1026: Privileged Account Management</u>	<div>  <u>1Panel, SUSE</u> </div>
CVE-2025-6018	T1068: Exploitation for Privilege Escalation	<u>DS0009: Process</u>	<u>M1038: Execution Prevention</u>	<div>  <u>SUSE, Debian</u> </div>
CVE-2025-7425	T1203: Exploitation for Client Execution	<u>DS0015: Application Log Content</u> , <u>DS0022: File Modification</u>	<u>M1048: Application Isolation and Sandboxing</u> , <u>M1051: Update Software</u>	<div>  <u>Red Hat, SUSE</u> </div> <div>  <u>Debian</u> </div>
CVE-2025-6000	T1203: Exploitation for Client Execution	<u>DS0022: File Modification</u> , <u>DS0029: Network Traffic Flow</u>	<u>M1051: Update Software</u>	<div>  <u>HashiCorp, SUSE</u> </div>
CVE-2025-5999	T1068: Exploitation for Privilege Escalation	<u>DS0009: Process Creation</u>	<u>M1050: Exploit Protection</u> , <u>M1051: Update Software</u>	<div>  <u>HashiCorp, SUSE</u> </div> <div>  <u>Red Hat</u> </div>

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-49796	T1499: Endpoint Denial of Service	DS0015: Application Log Content , DS0029: Network Traffic	M1037: Filter Network Traffic	 Red Hat , Debian , Rocky Linux , Ubuntu , Amazon Linux

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/excobalts-gored-the-silent-infiltrator-of-russian-sectors/>

<https://hivepro.com/threat-advisory/june-2025-linux-patch-roundup/>

<https://access.redhat.com/sites/default/files/attachments/cve-2019-11135--2019-11-12-1735.sh>

<https://access.redhat.com/articles/tsx-asynchronousabort>

<https://access.redhat.com/security/cve/cve-2019-19338>

<https://www.exploit-db.com/exploits/49766>

<https://www.wiz.io/blog/nvidia-ai-vulnerability-cve-2025-23266-nvidiascape>

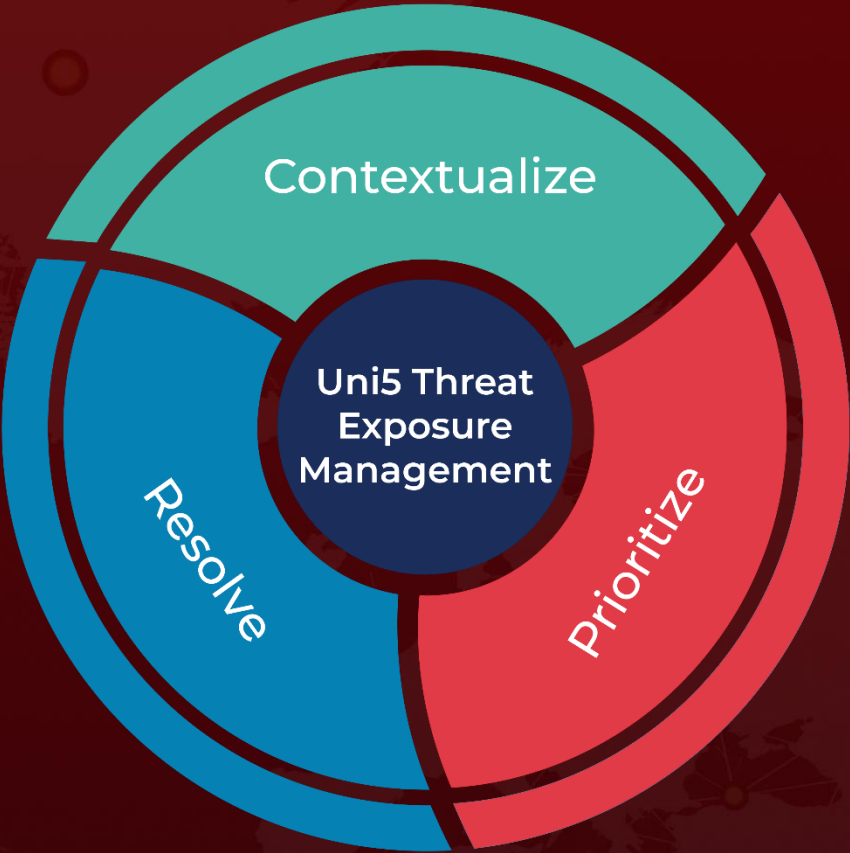
<https://github.com/advisories/GHSA-8j63-96wh-wh3j>

<https://cdn2.qualys.com/2025/06/17/suse15-pam-udisks-lpe.txt>

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
August 27, 2025 • 10:00 PM

