Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

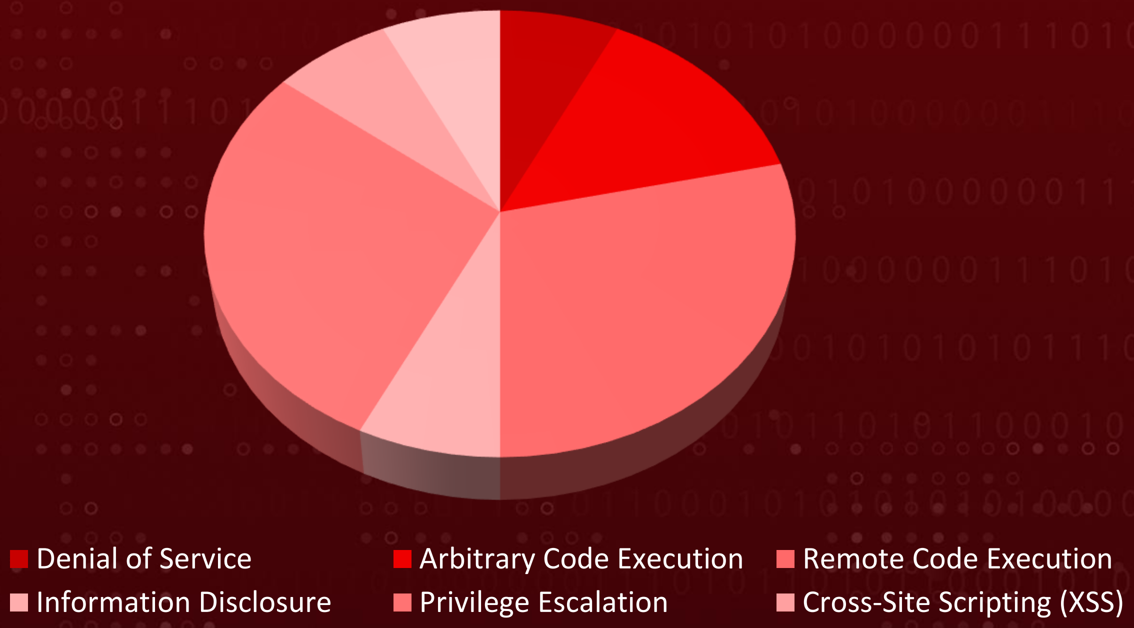
June 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
June 26, 2025	A1	TA2025199

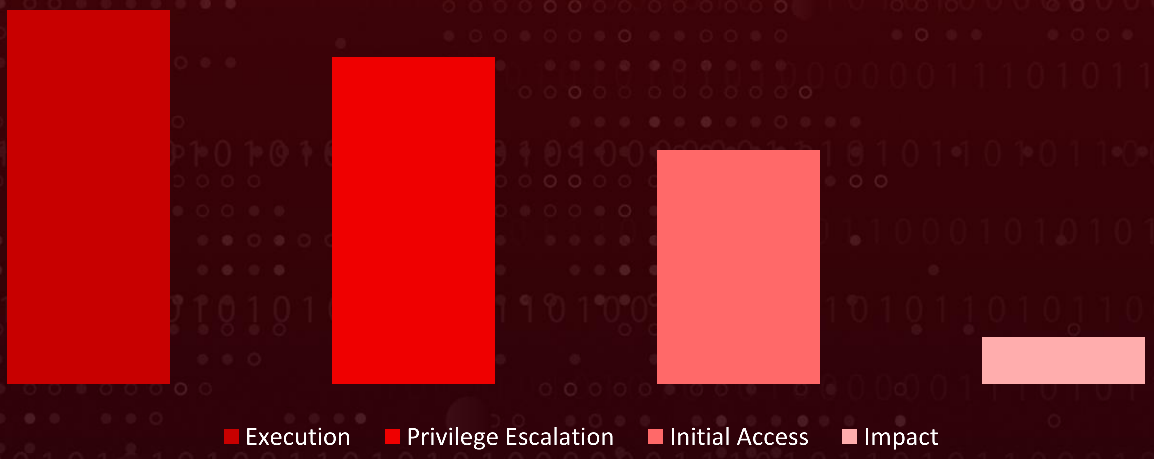
Summary

In June 159 new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, Red Hat, OpenSUSE, and Arch Linux. During this period, 2920 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 14 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-2025-27363*	FreeType Out-of-Bounds Write Vulnerability	FreeType, Ubuntu, SUSE, Debian, ALT Linux, Redhat, Amazon Linux, Oracle	Arbitrary code execution	Network
CVE-2025-37928	Linux Kernel dm-bufio Improper Scheduling Vulnerability	Linux Kernel, Debian, ALT Linux, SUSE, Redhat, Amazon Linux	Denial of Service	Local
CVE-2025-4123*	Grafana Cross-Site Scripting (XSS) Vulnerability	Grafana, ALT Linux, Redhat, SUSE, Debian, Oracle	Cross-Site Scripting (XSS)	Network
CVE-2025-49113	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube, Fedora, Debian, ALT Linux, Ubuntu	Remote Code Execution	Network
CVE-2025-4918*	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Firefox	Remote Code Execution	Network
CVE-2025-4919*	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Firefox	Remote Code Execution	Network
CVE-2025-5054	Ubuntu Apport Information Disclosure Vulnerability	ALT Linux Ubuntu	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-2025-5419*	Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	Chrome, Edge	Heap Corruption	Phishing
CVE-2025-6019	Libblockdev Privilege Escalation Vulnerability	ALT Linux, Redhat, Fedora, Ubuntu, Debian, Oracle, SUSE, Amazon Linux	Privilege Escalation	Local
CVE-2025-6018	Linux Pluggable Authentication Modules Local Privilege Escalation (LPE) vulnerability	SUSE, Debian	Privilege Escalation	Local
CVE-2025-6020	Linux PAM Privilege Escalation Vulnerability	Redhat, Fedora, Ubuntu, Amazon, SUSE, Debian, Oracle	Privilege Escalation	Local
CVE-2023-0386*	Linux Kernel Improper Ownership Management Vulnerability	ALT Linux, Netapp, Ubuntu	Privilege Escalation	Local
CVE-2025-47273	Python Setuptools Path Traversal Vulnerability	Setuptools, Fedora, SUSE, Ubuntu, Debian, ALT Linux, Redhat, Amazon	Remote Code Execution	Network
CVE-2025-4517	CPython Arbitrary Filesystem Write Vulnerability	SUSE, Python, Redhat, Amazon, Debian	Remote Code Execution	Network

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-2025-27363	✗	FreeType (FreeType) Version from 0.0.0 through 2.13.0	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:freetype:freetype:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:suse:suse:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:a:redhat:enterprise_linux:*:*:*:*:*:*:*:* cpe:2.3:o:amazon:linux:*:*:*:*:*:*:*:*	Paragon spyware
FreeType Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	FreeType Ubuntu SUSE Debian ALT Linux Redhat Amazon Linux Oracle

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4123	The Grafana Ghost	Grafana versionsPrior to 10.4.18+security-01, 11.2.9+security-01, 11.3.6+security-01, 11.4.4+security-01, 11.5.4+security-01, 11.6.1+security-01, and 12.0.0+security-01	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:grafana:grafana:*:*:*:*:*:*:*:* cpe:2.3:o:redhat:enterprise_linux:*:*:*:*:*:*:*:*	-
Grafana Cross-Site Scripting (XSS) vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-601 CWE-79	T1059: Command and Scripting Interpreter; T1059.007: JavaScript	Grafana ALT Linux Redhat SUSE Oracle ✗ Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4918	✗	Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*	-
Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-125	T1059: Command and Scripting Interpreter; T1059.007: JavaScript	Firefox 138.0.4 Firefox ESR 115.23.1 Firefox ESR 128.10.1 Thunderbird 138.0.2 Thunderbird 128.10.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-4919	✗	Mozilla Firefox Version Prior to 138.0.4, Firefox ESR Version Prior to 128.10.1, Firefox ESR Version Prior to 115.23.1	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mozilla:firefox:*:*:*:*:*:*:*:* cpe:2.3:a:mozilla:firefox_esr:*:*:*:*:*:*:*:*	-
Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787 CWE-125	T1189: Drive-by Compromise; T1059.007 Command and Scripting Interpreter: JavaScript; T1190 : Exploit Public-Facing Application	Firefox 138.0.4 Firefox ESR 115.23.1 Firefox ESR 128.10.1 Thunderbird 138.0.2 Thunderbird 128.10.2

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-5419	✗	Google Chrome prior to 137.0.7151.68 Microsoft Edge	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:a:microsoft:edge:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS

	CWE-787	T1190: Exploit Public-Facing Application;
		T1566: Phishing;
		T1059: Command and Scripting Interpreter
			Chrome
			Microsoft

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2023-0386	✗	Linux kernel versions prior to 6.2-rc6 (specifically 5.11 to <5.15.91; 5.16 to <6.1.9; 6.2:rc1 through 6.2:rc5)	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:o:suse:suse:*:*:*:*:*:*:*:*	-
Linux Kernel Improper Ownership Management Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-282	T1068: Exploitation for Privilege Escalation	ALT Linux Netapp Ubuntu

Vulnerability Details

#1 June witnessed a sweeping wave of security updates across the Linux ecosystem, with 2920 vulnerabilities addressed across various distributions and products. Remarkably, 159 of these flaws were released in last 30 days. HiveForce Lab has identified 16 critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon. These issues could grant attackers initial access, enable malicious code execution, facilitate evasion of security mechanisms, and allow privilege escalation, making immediate patching critical.

#2 One of the severe threats this month is CVE-2025-5419, a zero-day vulnerability in Google Chrome. This flaw involves an out-of-bounds read and write in Chrome’s V8 JavaScript engine, allowing remote attackers to exploit heap corruption via a specially crafted HTML page. Notably, this vulnerability is already being exploited in the wild. Meanwhile, Mozilla has patched two critical vulnerabilities in Firefox, CVE-2025-4918 and CVE-2025-4919, that were exploited before public disclosure. These flaws stem from how Firefox handles JavaScript promises and array math, potentially enabling attackers to manipulate memory, execute arbitrary code, or exfiltrate sensitive data.

#3 CVE-2025-27363, an out-of-bounds write vulnerability in the FreeType font rendering library that can lead to arbitrary code execution, has been actively exploited in Paragon spyware campaigns. Although a patch was released in March, the flaw continued to be exploited as recently as June.

#4 Another notable vulnerability is CVE-2025-4123, dubbed "The Grafana Ghost." This cross-site scripting (XSS) flaw in Grafana combines a client-side path traversal with an open redirect, enabling attackers to redirect victims to a malicious site that hosts a plugin capable of executing arbitrary JavaScript in the user’s browser. Additionally, Fedora issued a critical update (FEDORA-2025-551aed076e) addressing multiple vulnerabilities in Salt. These flaws could lead to privilege escalation and denial-of-service conditions if left unpatched.

#5 These developments underscore the importance of a proactive and vigilant security posture. Even older, seemingly dormant vulnerabilities can resurface and become dangerous if neglected. As adversaries refine their techniques, organizations must prioritize regular patch management, continuous vulnerability assessments, and robust defense mechanisms to stay ahead of evolving threats and reduce the attack surface.

Recommendations

Proactive Strategies:

Stay Ahead with Timely Patching: Keep your systems secure by applying updates as soon as they become available, with a focus on critical vulnerabilities like CVE-2025-27363, CVE-2025-4123, CVE-2025-4918, CVE-2025-4919, CVE-2025-5419, as well as those actively exploited. Where feasible, automate patch management to reduce delays and minimize the risk of human oversight.

Conduct Regular Vulnerability Assessments: Perform scheduled scans across all assets using both authenticated and unauthenticated methods to identify known vulnerabilities. Integrate threat intelligence feeds to dynamically prioritize vulnerabilities based on exploit availability and activity in the wild.

Stay One Step Ahead with Continuous Monitoring: Deploy vulnerability scanners and security monitoring tools to proactively identify unpatched systems, misconfigurations, and exploit attempts before attackers can take advantage of them. Continuous monitoring helps detect security gaps early, ensuring swift action to minimize risks.

Limit Exposure: Reduce the risk of lateral movement by restricting user and system permissions to only what’s necessary. Implement Zero Trust principles to enforce strict access controls, ensuring that even if an attacker breaches one part of the network, they can’t move freely to critical assets.

Reactive Strategies:

Detect and Block Threats in Real Time: Strengthen your defenses with Intrusion Detection and Prevention Systems (IDS/IPS) to identify and block exploitation attempts as they happen. Enhance security further with behavior-based anomaly detection, which flags suspicious activities before they escalate into full-blown attacks.

Empower Users to Defend Against Phishing Attacks: Since many cyber threats start with phishing emails and social engineering, equip your team with the knowledge to spot suspicious emails, deceptive links, and fraudulent attachments. Encourage strong authentication practices and caution against downloading untrusted files to prevent attackers from gaining a foothold in your network.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-27363*	T1059: Command and Scripting Interpreter; T1190: Exploit Public-Facing Application	DS0017:Command	M1051: Update Software	✓ FreeType Ubuntu SUSE Debian ALT Linux Redhat Amazon Linux Oracle
CVE-2025-37928	T1499.004: Application or System Exploitation	DS0015: Application Log	M1037: Filter Network Traffic	✓ Linux Kernel Debian ALT Linux SUSE ✗ Redhat Amazon Linux
CVE-2025-4123*	T1059.007: JavaScript	DS0017:Command DS0012: Script	M1038: Execution Prevention	✓ Grafana ALT Linux Redhat SUSE Oracle ✗ Debian
CVE-2025-49113	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	DS0017:Command	M1051: Update Software	✓ Roundcube Fedora Debian ALT Linux Ubuntu
CVE-2025-4918*	T1059: Command and Scripting Interpreter, T1059.007: JavaScript	DS0017:Command DS0012: Script	M1038: Execution Prevention	✓ Firefox 138.0.4 Firefox ESR 115.23.1 Firefox ESR 128.10.1 Thunderbird 138.0.2 Thunderbird 128.10.2

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-4919*	T1189: Drive-by Compromise T1059.007 Command and Scripting Interpreter: JavaScript T1190 : Exploit Public-Facing Application	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Firefox 138.0.4 Firefox ESR 115.23.1 Firefox ESR 128.10.1 Thunderbird 138.0.2 Thunderbird 128.10.2
CVE-2025-5054	T1068: Exploitation for Privilege Escalation	DS0009: Process	M1038: Execution Prevention	✓ ALT Linux Ubuntu
CVE-2025-5419*	T1190: Exploit Public-Facing Application, T1566: Phishing, T1059: Command and Scripting Interpreter	DS0017:Command	M1051: Update Software	✓ Chrome Microsoft
CVE-2025-6019	T1068: Exploitation for Privilege Escalation, T1548.001: Setuid and Setgid	DS0009: Process DS0017:Command	M1038: Execution Prevention M1028: Operating System Configuration	✓ ALT Linux Redhat Fedora Ubuntu Debian Oracle SUSE Amazon Linux
CVE-2025-6018	T1068: Exploitation for Privilege Escalation	DS0009: Process	M1038: Execution Prevention	✓ SUSE Debian
CVE-2025-6020	T1068: Exploitation for Privilege Escalation	DS0027: Driver	M1050: Exploit Protection	✓ Redhat Fedora Ubuntu SUSE Oracle ✗ Amazon Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2023-0386*	T1068: Exploitation for Privilege Escalation	DS0009: Process	M1050: Exploit Protection M1038: Execution Prevention	✓ ALT Linux Netapp Ubuntu
CVE-2025-47273	T1059: Command and Scripting Interpreter	DS0017:Command	M1038: Execution Prevention	✓ Setuptools Fedora Ubuntu Debian ALT Linux Amazon ✗ Redhat SUSE
CVE-2025-4517	T1059: Command and Scripting Interpreter; T1566: Phishing	DS0017:Command DS0029: Network Traffic	M1033: Limit Software Installation M1031: Network Intrusion Prevention	✓ Python Amazon Debian ✗ Redhat SUSE

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/

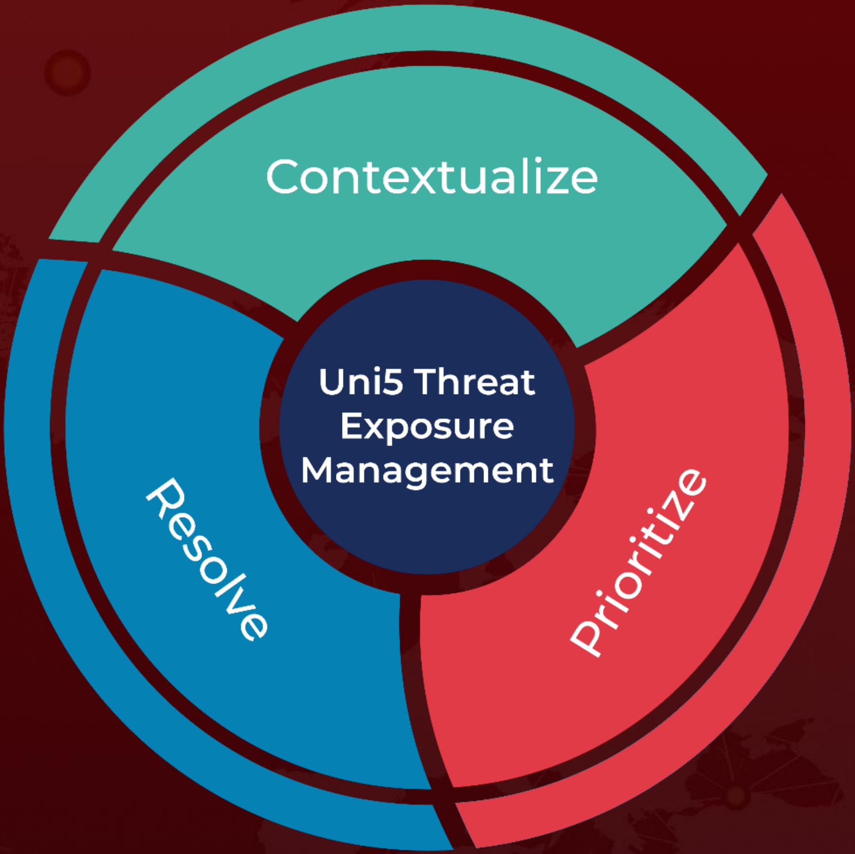
https://access.redhat.com/security/security-updates/

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

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

June 26, 2025 • 2:00 AM

More at www.hivepro.com