

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

March 2025 Linux Patch Roundup

Date of Publication

April 1, 2025

Admiralty Code

A1

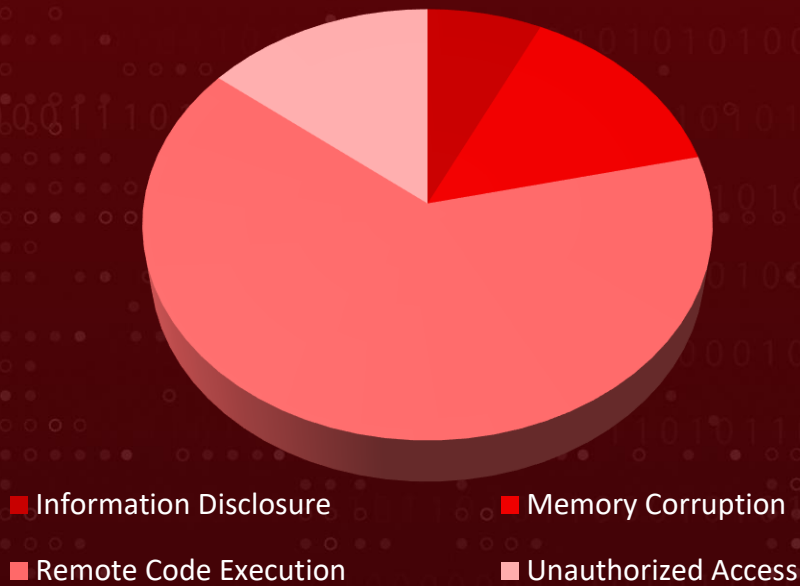
TA Number

TA2025098

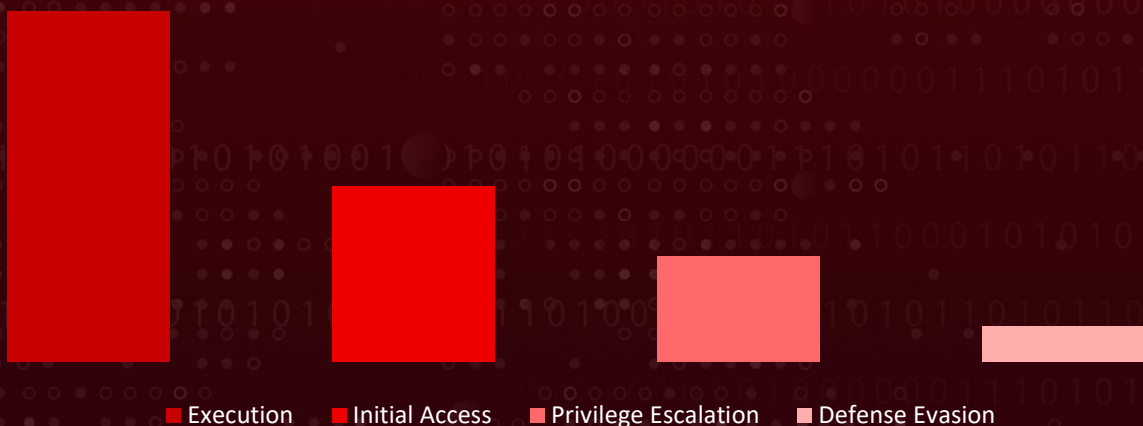
Summary

In March, 230 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, over 2000+ 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 11 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-2025-1942	Mozilla Firefox Information Disclosure Vulnerability	Thunderbird, Mozilla, FEDORA, Ubuntu, Debian, Suse, ALT Linux, Redhat	Memory Corruption and Unauthorized Access	Network
<u>CVE-2025-24813</u>	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat, Suse, Debian, Ubuntu, ALT Linux, Redhat, Amazon Linux	Remote Code Execution, Information Disclosure	Remote
<u>CVE-2025-1094*</u>	PostgreSQL psql SQL Injection Vulnerability	PostgreSQL, Debian, Redhat, Ubuntu, Suse,, ALT Linux, Oracle Linux, Amazon Linux	Code Execution	Network
<u>CVE-2025-24201*</u>	Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability	Apple iOS and iPadOS, Apple macOS Sequoia, Apple visionOS, Apple Safari, Chrome Microsoft, Suse, Redhat, Debian, Ubuntu, ALT Linux, Oracle Linu	Memory Corruption	Phishing
<u>CVE-2025-27363</u>	FreeType Out of Bounds Write Vulnerability	FreeType (FreeType), Debian, Ubuntu, Suse, ALT Linux, Redhat, Amazon Linux	Arbitrary Code Execution	Network
CVE-2025-27636	Apache Camel Header Injection Vulnerability	Apache Camel, Redhat, ALT Linux	Remote Code Execution, Unauthorized Access	Remote
CVE-2025-29891	Apache Camel Header Injection Vulnerability	Apache Camel, ALT Linux, Redhat	Remote Code Execution	Phishing




* 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
<u>CVE-2021-44228*</u>	Apache Log4j2 Remote Code Execution Vulnerability	Apache Log4j2, Ubuntu Suse, Redhat, Debian, ALT Linux, Amazon Linux	Arbitrary Code Execution	Network
<u>CVE-2021-45046*</u>	Apache Log4j2 Deserialization of Untrusted Data Vulnerability	Apache Log4j2, Debian, Ubuntu, Suse, Gentoo, Redhat, ALT Linux, Amazon Linux	Remote Code Execution	Network
<u>CVE-2022-35914*</u>	Teclib GLPI Remote Code Execution Vulnerability	GLPI, ALT Linux, RedOS	Remote Code Execution	Phishing
CVE-2024-8517	SPIP Command Injection Vulnerability	SPIP, Debian, Ubuntu, ALT Linux	Remote Code Execution	Remote



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-2025-1094*		PostgreSQL Versions Before 17.3, 16.7, 15.11, 14.16, and 13.19	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:postgresql:postgresql:*:*:*:*:*	-
PostgreSQL psql SQL Injection Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-149	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	Postgrespl Redhat Debian Ubuntu Suse ALT Linux Oracle Linux Amazon Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2025-24201*</u>		Apple iOS and iPadOS Versions before 18.3.2, Apple macOS Sequoia Versions before 15.3.2, Apple visionOS Version before 2.3.2, Apple Safari Version before 18.3.1	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:a:apple:visionos:*:*:*:*:* cpe:2.3:a:apple:safari:*:*:*:*:* cpe:2.3:a:apple:macos_sequoia:*:*:*:*:* cpe:2.3:a:apple:ios:*:*:*:*:	-
Apple Multiple Products WebKit Out-of-Bounds Write Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1497: Virtualization/Sandbox Evasion; T1190: Exploit Public-Facing Application	Apple Chrome Microsoft Suse Redhat Ubuntu ALT Linux Oracle Linux Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-44228*</u>	Log4shell	Apache Log4j2	Silk Typhoon, Flax Typhoon, Andariel, ExCobalt, Lazarus Group
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	<p>cpe:2.3:a:apache:log4j:*:*:*:*:*:*</p>	<p>Nosedive, Raptor Train, Atharvan, ELF Backdoor, Jupiter, MagicRAT, No Pineapple, TigerRAT, Valefor/VSingle, ValidAlpha, YamaBot, NukeSped, Goat RAT, Black RAT, AndarLoader, DurianBeacon, Trifaux, KaosRAT, Preft, Andariel Scheduled Task Malware, BottomLoader, NineRAT, DLang, Nestdoor , Artprint, Artshow, Blackcanvas, Deimosc2, Falsejade, Hiddengift, Hollowdime, Messyhelp, Pineapple, Quartzfire, Redthorn, Rifle, Sonicboom, SHATTEREDGLASS ransomware and MAUI Ransomware, GoRed Backdoor, FritzFrog Botnet, NineRAT, DLRAT, BottomLoader, HazyLoad, LockBit Ransomware, AvosLocker ransomware</p>
Apache Log4j2 Remote Code Execution Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-917	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<u>Ubuntu</u> <u>Suse</u> <u>Redhat</u> <u>Apache</u> <u>ALT Linux</u> <u>Amazon Linux</u> <u>Debian</u>

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2021-45046*</u>	Log4Shell 2	Apache log4j	Prophet Spider, MuddyWater
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:log4j:*:*:*:*:*:*:*:*	Mirai, Cobalt, Avos, Silver, NightSky, DrWeb, EnemyBot
Apache Log4j2 Deserialization of Untrusted Data Vulnerability			ASSOCIATED TTPs
	CWE ID	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	Debian Ubuntu Suse Gentoo Redhat Apache ALT Linux Amazon Linux
	CWE-917		

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2022-35914*</u>		GLPI through 10.0.2	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:glpi-project:glpi:*:*:*:*:*:*:*	-
Teclib GLPI Remote Code Execution Vulnerability			ASSOCIATED TTPs
	CWE ID	T1059: Command and Scripting Interpreter	ALT Linux RedOS GLPI
	CWE-74		

Vulnerability Details

#1

March brought a significant wave of security updates across the Linux ecosystem, addressing over 2,000 vulnerabilities in various distributions and products. Notably, 230 of these flaws were discovered in March alone, underscoring the ongoing battle against security threats. Researchers at HiveForce Lab have flagged eleven critical vulnerabilities, some of which are already being actively exploited, while others pose a high risk of future exploitation. These flaws enable attackers to gain initial access, execute malicious code, evade defenses, and escalate privileges, making immediate patching essential.

#2

Among the most concerning threats is CVE-2025-24201, a zero-day vulnerability in Apple's WebKit browser engine. This flaw has been actively exploited in sophisticated attacks, allowing cybercriminals to escape the Web Content sandbox through malicious web pages. Apple's latest patch strengthens earlier protections introduced in iOS 17.2, reinforcing defenses against this persistent exploit.

#3

Meanwhile, a high-severity SQL injection vulnerability (CVE-2025-1094) in PostgreSQL's psql tool has raised alarms. This flaw enables attackers to execute arbitrary SQL commands, potentially escalating to remote code execution (RCE) when combined with other exploits. In fact, chaining CVE-2025-1094 with CVE-2024-12356, a recently patched BeyondTrust software vulnerability, led to successful RCE in every tested scenario.

#4

Additionally, Red Hat recently issued a fresh patch for Log4Shell (CVE-2021-44228, CVE-2021-45046) in JBoss EAP. While Log4Shell was originally patched in 2021, hidden dependencies within JBoss may have continued using incomplete or vulnerable Log4j versions, prompting the need for additional security updates. Many enterprises still rely on older JBoss versions under long-term support (LTS), highlighting the importance of continuous security assessments.

#5

These developments serve as a stark reminder that even years-old vulnerabilities can resurface if left unaddressed. As cybercriminals continuously evolve their tactics, organizations must remain proactive in their security strategies. Regular patching, vulnerability monitoring, and robust security controls are critical to mitigating risks and staying ahead of emerging threats.

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-2025-24201 and CVE-2025-1094, as well as those actively exploited. Where feasible, automate patch management to reduce delays and minimize the risk of human oversight.



Secure Software Development & Dependency Management: Regularly audit third-party dependencies, especially in Java-based applications like JBoss EAP, where lingering Log4Shell risks could still pose a threat. Keep your software ecosystem secure by replacing outdated libraries, eliminating vulnerable components, and adhering to secure coding best practices to prevent exploitation.



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-2025-1942	T1203: Exploitation for Client Execution	<u>DS0015: Application Log</u>	<u>M1051: Update Software</u>	 <ul style="list-style-type: none"> Thunderbird Mozilla FEDORA Ubuntu Debian Suse ALT Linux Redhat
<u>CVE-2025-24813</u>	T1059: Command and Scripting Interpreter, T1068: Exploitation for Privilege Escalation	<u>DS0017: Command</u>	<u>M1045: Code Signing</u> <u>M1051: Update Software</u>	 <ul style="list-style-type: none"> Apache Suse Debian Ubuntu ALT Linux Redhat Amazon Linux
<u>CVE-2025-1094*</u>	T1190: Exploit Public-Facing Application, T1059: Command and Scripting Interpreter	<u>DS0009: Process</u> <u>DS0017: Command</u>	<u>M1051: Update Software</u> <u>M1030: Network Segmentation</u>	 <ul style="list-style-type: none"> Postgrespl Redhat Debian Ubuntu Suse ALT Linux Oracle Linux Amazon Linux
<u>CVE-2025-24201*</u>	T1497: Virtualization/Sandbox Evasion, T1190: Exploit Public-Facing Application	<u>DS0017: Command</u>	<u>M1048: Application Isolation and Sandboxing</u> <u>M1051: Update Software</u>	 <ul style="list-style-type: none"> Apple Chrome Microsoft Suse Redhat Ubuntu ALT Linux Oracle Linux Debian
<u>CVE-2025-27363</u>	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<u>DS0017: Command</u>	<u>M1051: Update Software</u>	 <ul style="list-style-type: none"> Freetype Debian Ubuntu Suse ALT Linux Redhat Amazon Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-27636	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1202 : Indirect Command Execution	<u>DS0029: Network Traffic</u> <u>DS0017: Command</u>	<u>M1050: Exploit Protection</u>	 <u>Apache</u> <u>Redhat</u> <u>ALT Linux</u>
CVE-2025-29891	T1190: Exploit Public-Facing Application, T1068: Exploitation for Privilege Escalation, T1202: Indirect Command Execution	<u>DS0029: Network Traffic</u>	<u>M1050: Exploit Protection</u>	 <u>Apache</u> <u>ALT Linux</u> <u>Redhat</u>
<u>CVE-2021-44228*</u>	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<u>DS0017: Command</u> <u>DS0015: Application Log</u>	<u>M1049: Antivirus/Antimalware</u> <u>M1051: Update Software</u>	 <u>Ubuntu</u> <u>Suse</u> <u>Redhat</u> <u>Debian</u> <u>Apache</u> <u>ALT Linux</u> <u>Amazon Linux</u>
<u>CVE-2021-45046*</u>	T1059: Command and Scripting Interpreter, T1190: Exploit Public-Facing Application	<u>DS0017: Command</u> <u>DS0015: Application Log</u>	<u>M1049: Antivirus/Antimalware</u> <u>M1051: Update Software</u>	 <u>Ubuntu</u> <u>Suse</u> <u>Gentoo</u> <u>Redhat</u> <u>Apache</u> <u>ALT Linux</u> <u>Amazon Linux</u> <u>Debian</u>
<u>CVE-2022-35914*</u>	T1059: Command and Scripting Interpreter	<u>DS0017: Command</u>	<u>M1051: Update Software</u>	 <u>ALT Linux</u> <u>RedOS</u> <u>GLPI</u>
CVE-2024-8517	T1059: Command and Scripting Interpreter	<u>DS0017: Command</u>	<u>M1051: Update Software</u>	 <u>Debian</u> <u>Ubuntu</u> <u>ALT Linux</u> <u>SPIP</u>

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/>

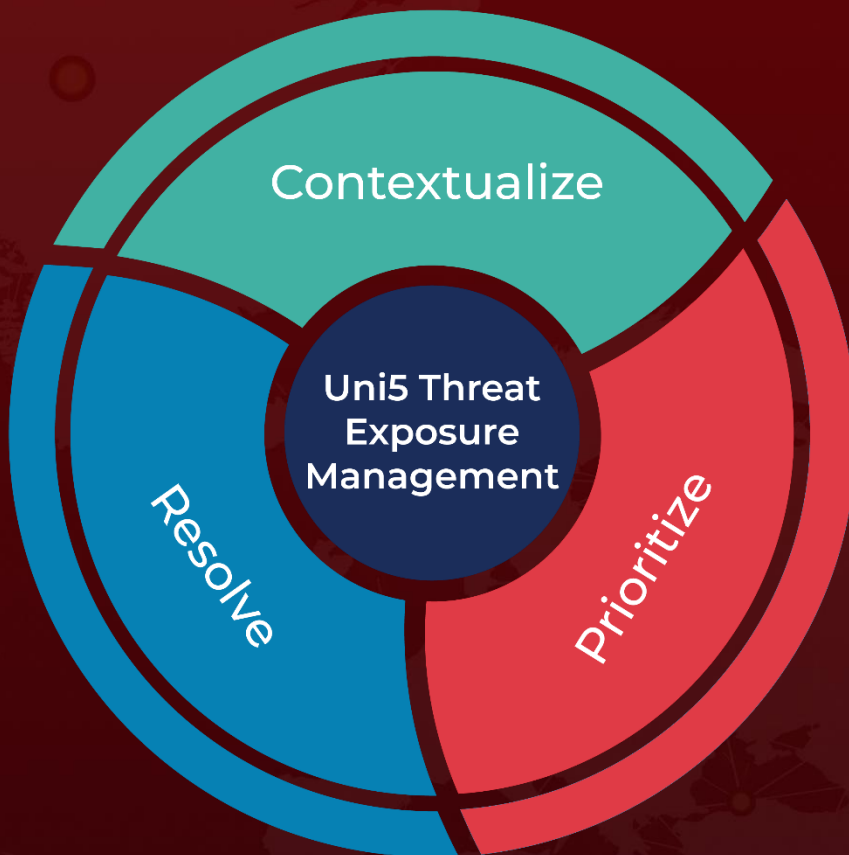
<https://access.redhat.com/security/security-updates/>

<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

April 1, 2025 • 8:50 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com