Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

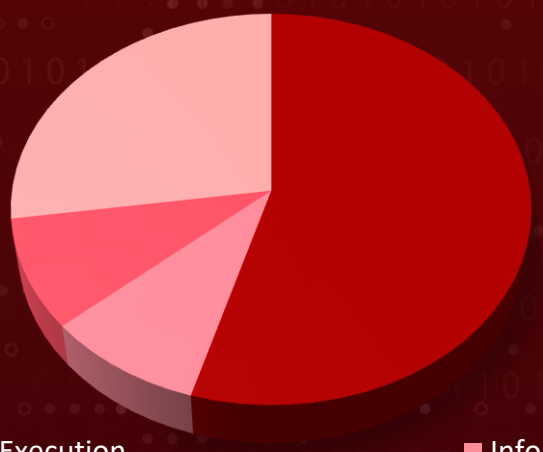
February 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
February 23, 2025	A1	TA2025055

Summary

In February, more than 157 new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, Fedora, OpenSUSE, and ALT Linux. During this period, over 1,400 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 which are exploited or have 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



Code Execution
Information Disclosure
Privilege Escalation
Unauthorized Access

Adversary Tactics

Execution
Initial Access
Privilege Escalation
Defense Evasion

CVEs

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-0444	Chromium Skia Use After Free Vulnerability	Chromium, Google Chrome, SUSE, Debian, Fedora, ALT Linux, Ubuntu	Code Execution	Phishing
CVE-2025-0445	Chromium V8 Use After Free Vulnerability	Chromium, Google Chrome, SUSE, Debian, Fedora, ALT Linux, Ubuntu	Code Execution	Phishing
CVE-2025-0451	Google Chrome Extensions API UI Spoofing Vulnerability	Chromium, Google Chrome, SUSE, Debian, Fedora, ALT Linux, Ubuntu	Unauthorized Access	Phishing
CVE-2025-1015	Thunderbird Cross-site Scripting Vulnerability	Thunderbird, Red Hat, SUSE, Debian, Fedora, ALT Linux, Ubuntu, Oracle Linux	Code Execution	Network
CVE-2025-26465*	OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability	OpenSSH Server, Red Hat, SUSE, Debian, Fedora, ALT Linux, Ubuntu	Unauthorized Access	Network
CVE-2024-53104*	Linux Kernel Out-of-Bounds Write Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, ALT Linux, Red Hat	Information Disclosure	Local
CVE-2025-1016	Mozilla Firefox Memory Safety Vulnerability	Firefox, Thunderbird, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux	Code Execution	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-2025-1017	Mozilla Firefox Memory Safety Vulnerability	Firefox, Thunderbird, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux	Code Execution	Network
CVE-2025-1009	Mozilla Firefox and Thunderbird Use After Free Vulnerability	Firefox, Thunderbird, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux, Amazon Linux	Code Execution	Phishing
CVE-2025-1020	Mozilla Firefox Memory Safety Vulnerability	Firefox, Firefox ESR Thunderbird, Debian, Ubuntu, SUSE, ALT Linux, Red Hat	Code Execution	Phishing
CVE-2025-24786	WhoDB Path Traversal Vulnerability	WhoDB, SUSE	Unauthorized Access	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-2025-26465	✗	OpenSSH versions 6.8p1 to 9.9p1, Red Hat, SUSE, Debian, Fedora, ALT Linux, Ubuntu	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:openssh:openssh:*:*:*:*:*:*:*:*	-
OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability	✗		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-390	T1203: Exploitation for Client Execution T1656: Impersonation	OpenSSH, Debian, Ubuntu, SUSE, ALT Linux, Red Hat

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53104	✗	Linux Kernel, Debian, Ubuntu, SUSE, ALT Linux, Red Hat	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:suse:*:*:*:*:*:*:*:*:* cpe:2.3:o:opensuse:leap:*:*:*:*:*:*:*:* cpe:2.3:o:fedoraproject:fedora:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1204: User Execution T1068: Exploitation for Privilege Escalation	Debian, Fedora, RedHat, Ubuntu, macOS

Vulnerability Details

#1 In February, the Linux ecosystem addressed 1,400+ vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and remote code execution. Additionally, 157 newly discovered vulnerabilities were patched. HiveForce Lab has identified 11 critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon.

#2 These vulnerabilities facilitate adversarial tactics such as Initial Access, Execution, Privilege Escalation, and Defense Evasion. Notably, two of these vulnerabilities are under active exploitation, requiring immediate attention and remediation.

#3 In Google Chrome, two high-severity use-after-free vulnerabilities (CVE-2025-0444, CVE-2025-0445) were discovered in Skia and the V8 JavaScript Engine, respectively. Attackers can exploit these flaws by luring users to malicious websites, leading to arbitrary code execution, system compromise, and data theft. Additionally, CVE-2025-0451 affects the Extensions API, enabling UI spoofing attacks, where adversaries manipulate browser elements to trick users into revealing sensitive information or performing unintended actions.

#4 The OpenSSH Client contains CVE-2025-26465, a flaw that allows machine-in-the-middle (MITM) attacks when the VerifyHostKeyDNS option is enabled. Attackers can exploit this weakness to intercept or modify SSH communications, putting confidential data and authentication security at risk. This is particularly concerning for system administrators and organizations relying on SSH for remote management.

#5 A critical vulnerability in the Linux kernel (CVE-2024-53104) affects the USB Video Class (UVC) driver, where an out-of-bounds write can lead to memory corruption, privilege escalation, or system crashes. Local attackers with access to a vulnerable system could exploit this flaw to gain elevated privileges or disrupt system stability.

#6 In Mozilla Firefox and Thunderbird, multiple vulnerabilities, including cross-site scripting (XSS), memory safety issues, and use-after-free flaws, have been discovered. These security flaws allow attackers to execute arbitrary code, crash applications. Successful exploitation may result in phishing attacks, data breaches, or full system compromise, highlighting the critical need for immediate patching. These vulnerabilities underscore the urgency of applying security updates to prevent potential exploitation and system compromise.

Recommendations

Proactive Strategies:

Exposure Assessment: Conduct an extensive service exposure evaluation with context of active threats to identify any publicly accessible services that may be vulnerable to exploitation. Following this assessment, it is essential to take immediate and decisive action to remediate any identified vulnerabilities by either installing necessary patches or implementing appropriate security measures. This proactive approach will help mitigate potential risks and enhance overall security posture.

User awareness is essential in defending against initial access threats, particularly in light of recent chromium vulnerabilities that require user execution for successful exploitation. These vulnerabilities highlight the importance of educating users about phishing and the identification of malicious activities. Organizations can stay one step ahead of cyber threats by fostering a culture of security hygiene.

Regular Patch Management & Kernel Updates Ensure Linux distributions, kernel versions, and installed packages are updated to the latest security patches. Automated updates should be configured using tools like unattended-upgrades, DNF Automatic, or apt-cron to prevent exploitation of known vulnerabilities.

Access Control & Least Privilege Implementation Enforce SELinux or AppArmor policies to restrict process permissions and prevent privilege escalation. Implement sudo with least privilege access, disable unnecessary services, and restrict root login to reduce attack surfaces.

Reactive Strategies:

Monitor endpoints for unusual library loads, as this can indicate potential threats. Utilizing EDR solutions can aid in detecting and mitigating code execution risks.

In case of system compromise, immediately isolate it from the network to prevent further spread. Use iptables or nftables to block malicious traffic and revoke credentials of affected users. Restore from a clean, verified backup to ensure system integrity before reconnecting to the network.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-0444	T1189:Drive-by Compromise T1203: Exploitation for Client Execution	DS0015: Application Log DS0029: Network Traffic	M1068: Execution Prevention	Debian, Fedora, Ubuntu, SUSE, ALT Linux, Chrome, Chromium
CVE-2025-0445	T1189:Drive-by Compromise T1203: Exploitation for Client Execution	DS0015: Application Log DS0029: Network Traffic	M1068: Execution Prevention	Debian, Fedora, Ubuntu, SUSE, ALT Linux, Chrome, Chromium
CVE-2025-0451	T1566: Phishing T1176: Browser Extensions T1204: User Execution	DS0015: Application Log DS0029: Network Traffic DS0009: Process	M1054: Software Configuration M1017: User Training	Debian, Fedora, Ubuntu, SUSE, ALT Linux, Chrome, Chromium
CVE-2025-1015	T1189: Drive-by Compromise T1204.001 User Execution: Malicious Link T1059.007: Command and Scripting Interpreter: JavaScript	DS0029: Network Traffic DS0009: Process DS0017: Command Execution	M1017: User Training M1021:Restrict Web-Based Content	Mozilla, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux
CVE-2025-26465	T1203: Exploitation for Client Execution T1656: Impersonation	DS0015: Application Log Content	M1051: Update Software M1017: User Training	OpenSSH, Debian, Ubuntu, SUSE, ALT Linux, Red Hat
CVE-2024-53104	T1204: User Execution T1068: Exploitation for Privilege Escalation	DS0009: Process DS0008: Kernel	M1051: Update Software	Debian, Ubuntu, SUSE, ALT Linux, Red Hat

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-1016	T1203: Exploitation for Client Execution	DS0009: Process DS0017: Command Execution	M1038: Execution Prevention	Mozilla, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux
CVE-2025-1017	T1203: Exploitation for Client Execution	DS0009: Process DS0017: Command Execution	M1038: Execution Prevention	Mozilla, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux
CVE-2025-1009	T1189: Drive-by Compromise T1566: Phishing T1203: Exploitation for Client Execution	DS0017: Command Execution DS0015: Application Log Content	M1038: Execution PreventionM1017: User Training	Mozilla, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux, Amazon Linux
CVE-2025-1020	T1566: Phishing T1203: Exploitation for Client Execution	DS0017: Command Execution DS0009: Process Creation	M1038: Execution Prevention M1040: Behavior Prevention on Endpoint M1017: User Training	Mozilla, Debian, Ubuntu, SUSE, ALT Linux, Red Hat
CVE-2025-24786	T1068: Exploitation for Privilege Escalation	DS0009: Process	M1051: Update Software	SUSE, WhoDB

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/

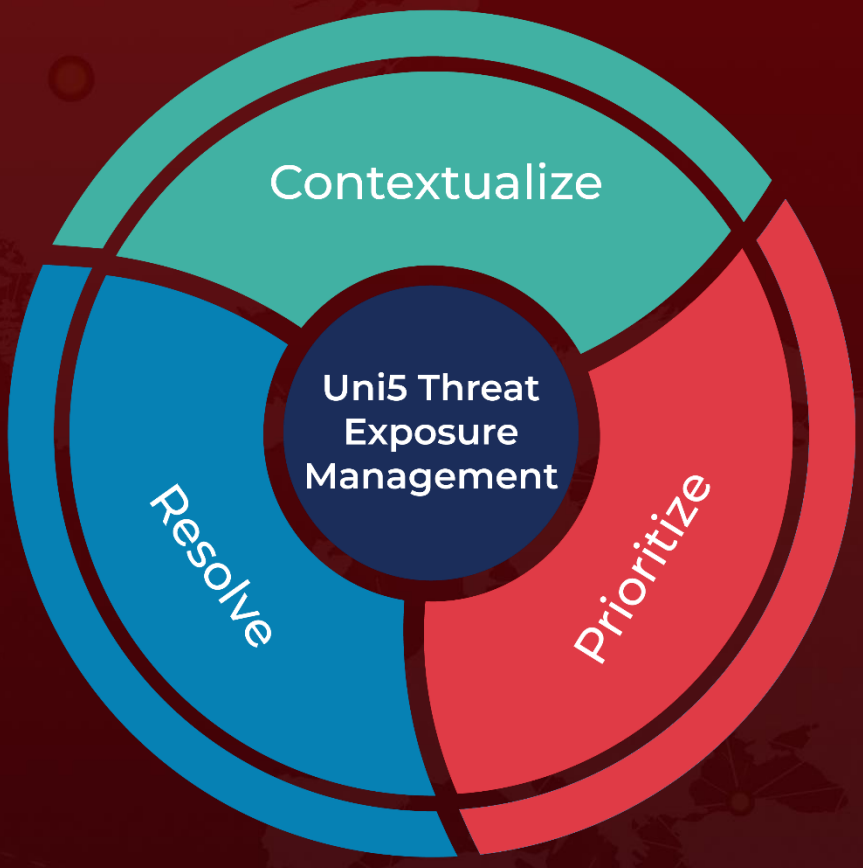
https://access.redhat.com/security/security-updates/

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

February 23, 2025 • 09:00 PM

More at www.hivepro.com