Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

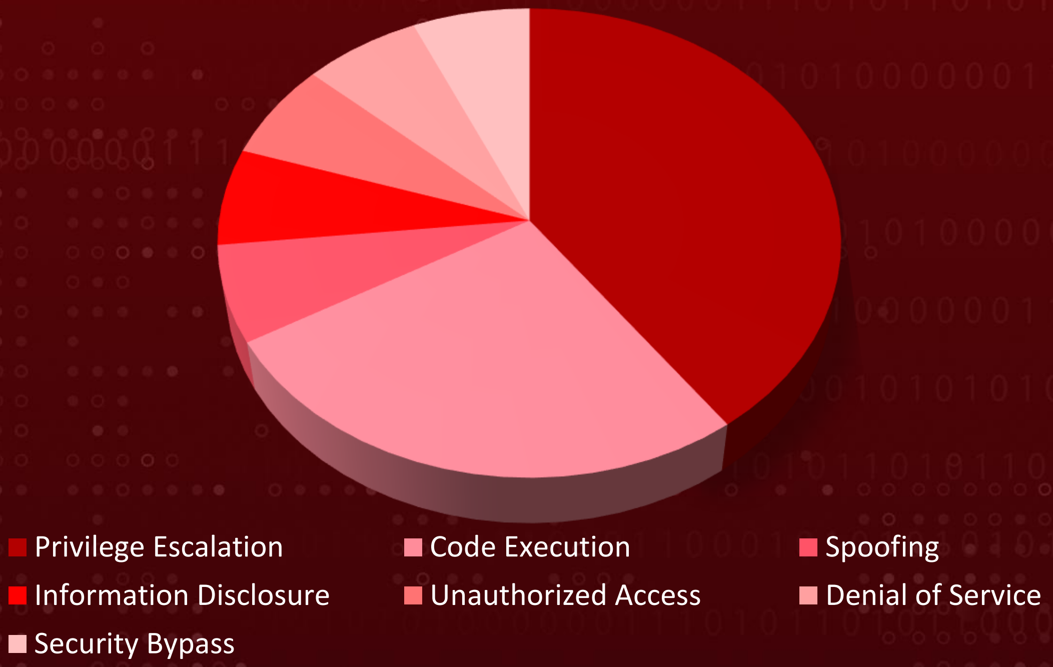
May 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
May 28, 2025	A1	TA2025165

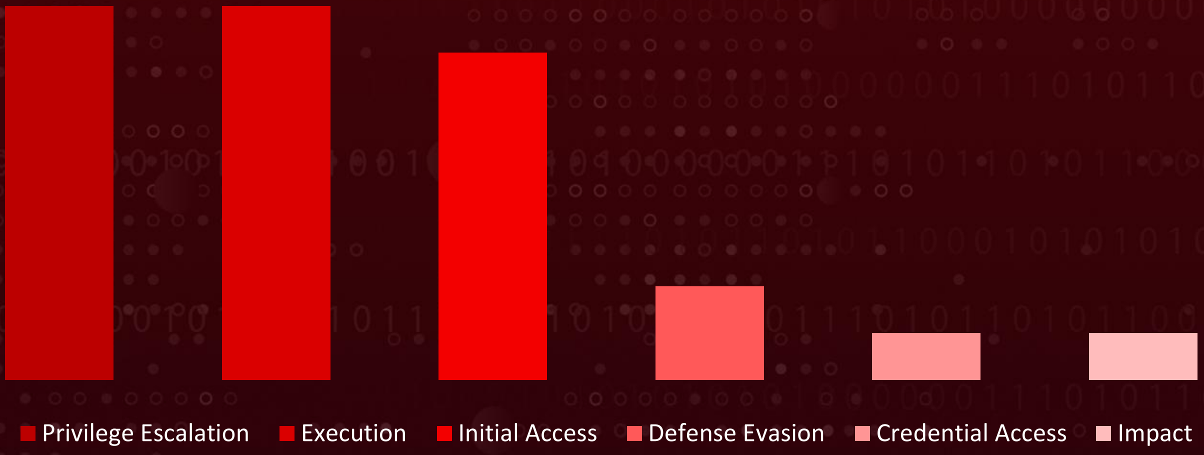
Summary

In May, more than 335 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 2500 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 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



Adversary Tactics



CVEs

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-4664*	Chromium Loader Insufficient Policy Enforcement Vulnerability	Chromium, Google Chrome, Microsoft Edge	Information Disclosure	Phishing
CVE-2025-4052	Chromium DevTools Inappropriate implementation Vulnerability	Chromium, Google Chrome	Unauthorized Access	Phishing
CVE-2025-4083	Mozilla Firefox Improper Isolation or Compartmentalization Vulnerability	Mozilla Firefox	Privilege Escalation	Network
CVE-2025-31651	Apache Tomcat Improper Neutralization Vulnerability	Apache Tomcat, Red Hat, SUSE, Debian, Amazon Linux, Ubuntu	Unauthorized Access	Remote
CVE-2025-2866	LibreOffice Improper Verification of Cryptographic Signature Vulnerability	LibreOffice, Red Hat, SUSE, Debian, Ubuntu	Spoofing	Local
CVE-2025-43859	h11 HTTP Request Smuggling Vulnerability	h11, Red Hat, SUSE, Debian, Fedora, Ubuntu	Unauthorized Access	Remote
CVE-2025-4919*	Mozilla Firefox Out-of-Bounds Read or Write Vulnerability	Mozilla Firefox	Privilege Escalation	Remote

* 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-2025-3028	Mozilla Firefox Use-After-Free Vulnerability	Mozilla Firefox	Code Execution	Network
CVE-2025-21756	Linux Kernel Use-After-Free Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Amazon Linux, Oracle Linux	Privilege Escalation	Local
CVE-2025-21655	Linux Kernel Eventfd RCU Period Handling Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, Red Hat, Amazon Linux	System Instability	Local
CVE-2025-32433	Erlang/OTP Unauthenticated Remote Code Execution Vulnerability	Erlang/OTP, Debian, Ubuntu, SUSE, ALT Linux, Amazon Linux	Code Execution	Remote
CVE-2025-21704	Linux Kernel Memory Corruption Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE	Memory Corruption	Local
CVE-2025-31650	Apache Tomcat Improper Input Validation Vulnerability	Apache Tomcat, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Amazon Linux	Denial of Service	Remote
CVE-2025-37899	Linux Kernel Use-After-Free Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE	Privilege Escalation	Local

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-2025-4664	✗	Google Chromium, 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 Loader Insufficient Policy Enforcement Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-346	T1528: Steal Application Access Token; T1189 : Drive-by Compromise; T1204: User Execution	https://www.google.com/intl/en/chrome/?standalone=1; https://www.microsoft.com/en-us/edge/download?form=MA13FW

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	https://www.mozilla.org/en-US/firefox/138.0.4/releasenotes/ https://www.mozilla.org/en-US/firefox/128.10.1/releasenotes/ https://www.mozilla.org/en-US/firefox/115.23.1/releasenotes/

Vulnerability Details

#1 In May, the Linux ecosystem addressed 2500+ vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and remote code execution. Additionally, 335 newly discovered vulnerabilities were patched. HiveForce Lab has identified 14 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 Starting with Google Chrome, the most critical fix is for CVE-2025-4664, a zero-day vulnerability that has been actively exploited. This flaw in Chrome's Loader component allows malicious web pages to leak cross-origin data, including sensitive information like session tokens or OAuth credentials.

#4 Mozilla Firefox and Thunderbird received several security patches, the most notable being CVE-2025-4919, another actively exploited vulnerability. This bug allows out-of-bounds read and write operations due to incorrect JavaScript array index handling. Other patched issues include CVE-2025-4083, a flaw in process isolation that could allow malicious code to escape its intended sandbox, and CVE-2025-3028, a use-after-free bug involving XSLTProcessor and JavaScript.

#5 The Python HTTP library h11 is impacted by CVE-2025-43859, a vulnerability in how chunked transfer encoding is parsed. This flaw can lead to HTTP request smuggling when deployed behind tolerant reverse proxies. It’s been patched in version 0.16.0, and developers relying on h11 should update dependencies as soon as possible.

#6 Finally, several vulnerabilities were fixed in core Linux components, although none of these have been reported as actively exploited at the time of publication. These include CVE-2025-21655, CVE-2025-21704, CVE-2025-21756, and CVE-2025-37899. The nature of these issues ranges from local privilege escalation to potential denial-of-service conditions. 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.

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.

Harden Browser and Web-Facing Applications: Since multiple browser-based and web infrastructure vulnerabilities were disclosed, ensure all browsers, email clients, and web applications are updated and securely configured. Consider using automatic update mechanisms where available and enforce usage of supported versions only.

Review and Secure Software Dependencies: For development environments, ensure libraries and components (e.g., Python packages, HTTP parsers, cryptographic tools) are up to date. Vulnerabilities in common libraries can cascade into larger application-level risks.

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:

Deploy or tighten endpoint detection and response (EDR), SIEM rules, and network traffic analysis to detect late-stage exploitation attempts or persistence mechanisms. Focus on web, browser, and script-related anomalies.

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-2025-4664	T1189:Drive-by Compromise T1528 : Steal Application Access Token T1204: User Execution	DS0015: Application Log DS0029: Network Traffic	M1068: Execution Prevention M1051: Update Software	✓ Chrome, Chromium, Edge
CVE-2025-4052	T1204: User Execution T1068: Exploitation for Privilege Escalation	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1017: User Training M1050: Exploit Protection	✓ Chrome, Chromium
CVE-2025-4083	T1204: User Execution T1068: Exploitation for Privilege Escalation	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1017: User Training M1050: Exploit Protection	✓ Mozilla
CVE-2025-31651	T1068: Exploitation for Privilege Escalation T1190 : Exploit Public-Facing Application	DS0009: Process DS0029: Network Traffic	M1051: Update Software M1050: Exploit Protection	✓ Apache Tomcat, Debian, Ubuntu, SUSE, Amazon Linux, Red Hat
CVE-2025-2866	T1218: System Binary Proxy Execution T1566: Phishing	DS0015: Application Log Content DS0009: Process	M1017: User Training M1047: Audit	✓ LibreOffice, Debian, Ubuntu, SUSE, Red Hat
CVE-2025-43859	T1190 : Exploit Public-Facing Application T1027 : Obfuscated Files or Information	DS0009: Process DS0029: Network Traffic	M1040: Behavior Prevention on Endpoint	✓ h11, Debian, Ubuntu, SUSE, Fedora, Red Hat

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	✓ Mozilla
CVE-2025-3028	T1189: Drive-by Compromise T1059.007 Command and Scripting Interpreter: JavaScript T1190 : Exploit Public-Facing Application	DS0029: Network Traffic DS0015: Application Log	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Mozilla
CVE-2025-21756	T1068: Exploitation for Privilege Escalation	DS0009: Process DS0008: Kernel	M1051: Update Software M1038: Execution Prevention	✓ Linux Kernel, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Oracle Linux, Amazon Linux
CVE-2025-21655	T1068: Exploitation for Privilege Escalation	DS0009: Process DS0008: Kernel	M1051: Update Software M1038: Execution Prevention	✓ Linux Kernel, Debian, Ubuntu, SUSE, Amazon Linux, Red Hat

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-32433	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter T1068: Exploitation for Privilege Escalation	DS0009: Process DS0017: Command Execution DS0029: Network Traffic	M1038: Execution Prevention M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Erlang/OTP, Debian, Ubuntu, SUSE, ALT Linux, Amazon Linux
CVE-2025-21704	T1068: Exploitation for Privilege Escalation T1204: User Execution	DS0009: Process DS0008: Kernel	M1051: Update Software M1038: Execution Prevention	✓ Linux Kernel, Debian, Ubuntu, SUSE
CVE-2025-31650	T1499: Endpoint Denial of Service T1190: Exploit Public-Facing Application	DS0009: Process DS0015: Application Log	M1050: Exploit Protection M1038: Execution Prevention	✓ Apache Tomcat, Debian, Ubuntu, SUSE, ALT Linux, Red Hat, Amazon Linux
CVE-2025-37899	T1068: Exploitation for Privilege Escalation T1203: Exploitation for Client Execution	DS0009: Process DS0008: Kernel DS0029: Network Traffic	M1051: Update Software M1038: Execution Prevention M1050: Exploit Protection	✓ Linux Kernel, Debian, Ubuntu, 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/

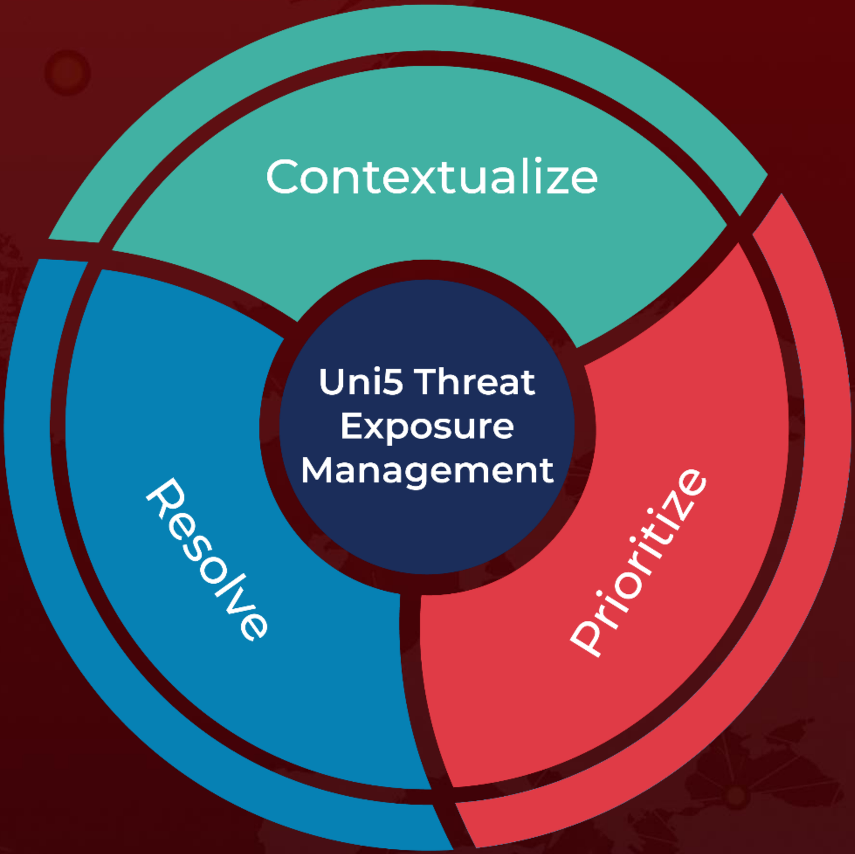
https://access.redhat.com/security/security-updates/

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

May 28, 2025 • 6:30 AM

More at www.hivepro.com