Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

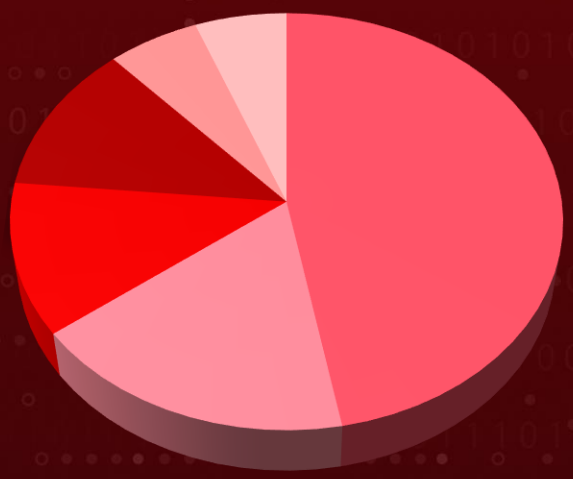
July 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
July 25, 2025	A1	TA2025233

Summary

In July, more than **1217** 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 **2389** 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 17 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



- Code Execution
- Security Bypass
- Privilege Escalation
- Denial of Service
- Information Disclosure
- Cross-Site Scripting (XSS)

Adversary Tactics

- Execution
- Initial Access
- Privilege Escalation
- Impact

CVEs

CVE	NAME	AFFECTED PRODUCT	Impact	Attack Vector
CVE-2025-32023	Redis Hyperloglog Out-of-Bounds Write Vulnerability	Redis, Debian, Red Hat, Amazon Linux, Alpine, Linux Oracle	Remote Code Execution	Local
CVE-2025-32462	Sudo Local Privilege Escalation Vulnerability	Sudo stable (v1.9.0 – 1.9.17) and legacy (v1.8.8 – 1.8.32) versions, Alpine Linux, Ubuntu, Debian, openSUSE, Fedora	Privilege Escalation	Local
CVE-2025-32463	Sudo Local Privilege Escalation Vulnerability	Sudo versions 1.9.14 to 1.9.17, Red Hat, Ubuntu, Debian, openSUSE, Alpine Linux	Privilege Escalation	Local
CVE-2025-38089	Linux Kernel Remote Denial Of Service Vulnerability	Linux kernel, Debian, Ubuntu, Red Hat, Oracle Linux	Denial of Service	Network
CVE-2025-48384	Git CLI Arbitrary File Write Vulnerability	Git, Ubuntu, Red Hat, Debian, Alpine Linux	Arbitrary File Write	Network
CVE-2025-53367	DjVuLibre Out-of-Bounds Write Vulnerability	DjVuLibre prior to version 3.5.29, Debian, Ubuntu, Fedora	Local Code Execution	Phishing
CVE-2025-6554*	Google Chromium V8 Type Confusion Vulnerability	Google Chrome prior to 138.0.7204.96, Microsoft Edge, Debian	Remote 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-2025-6558*	Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	Google Chrome prior to 138.0.7204.157, Debian, Microsoft Edge	Unauthorized Access	Network
CVE-2025-6424	Mozilla Firefox ESR Use-After-Free Vulnerability	Mozilla Firefox, Thunderbird, Debian, Ubuntu, Red Hat, openSUSE, Amazon Linux, Oracle Linux	Remote Code Execution	Network
CVE-2025-23048	Apache HTTP Server Vulnerability	Apache HTTP Server 2.4.35 through to 2.4.63, Red Hat, Ubuntu, Debian	Access Control Bypass	Network
CVE-2025-6427	Mozilla Firefox Content Security Policy Bypass via Subdocument Manipulation Vulnerability	Mozilla Firefox versions prior to 140, openSUSE, Debian	Security Restriction Bypass	Network
CVE-2025-38001	Linux Kernel Use-After-Free Vulnerability	Linux Kernel, Debian, Ubuntu, Red Hat, openSUSE, Amazon Linux, Oracle Linux	Denial of Service	Local
CVE-2025-48988	Apache Tomcat Unrestricted Resource Allocation Vulnerability	Apache Tomcat, Debian, Red Hat, openSUSE, Amazon Linux	Denial of Service	Network
CVE-2025-5222	Internationl components for unicode (ICU) Stack Buffer Overflow Vulnerability	Debian, Ubuntu, Red Hat, openSUSE, Amazon Linux	Memory Corruption	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-2024-38475*	Apache HTTP Server Improper Escaping of Output Vulnerability	Apache, Red Hat, openSUSE, Amazon Linux, Oracle Linux, Ubuntu, Debian	Remote Code Execution	Network
CVE-2019-5418*	Rails Ruby on Rails Path Traversal Vulnerability	Rails, openSUSE, Ubuntu, Red Hat, Debian	Information Disclosure	Network
CVE-2024-42009*	RoundCube Webmail Cross-Site Scripting Vulnerability	RoundCube Version Prior to 1.6.8 and 1.5.8, Debian, Ubuntu, openSUSE	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.

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-2025-6554	✗	Google Chrome prior to 138.0.7204.96, Microsoft Edge, Debian	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:* cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:*:*:*	-
Google Chromium V8 Type Confusion Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-843	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation	Google Chrome, Microsoft Edge, Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-6558	✗	Google Chrome prior to 138.0.7204.157, Debian, Microsoft Edge	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium ANGLE and GPU Improper Input Validation Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-20	T1497: Virtualization/Sandbox Evasion, T1189: Drive-by Compromise	Google Chrome, Debian, Microsoft Edge

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-38475	✗	Apache SMA 100 Series (SMA 200, 210, 400, 410, 500v) Version 10.2.1.13-72sv and earlier versions, Red Hat, openSUSE, Amazon Linux, Oracle Linux, Ubuntu, Debian	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:sonicwall:sma_firmware:*:*:*:*:*:*:*:* cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*	-
Apache HTTP Server Improper Escaping of Output Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-116	T1190: Exploit Public-Facing, Application; T1059: Command and Scripting Interpreter	Apache, Ubuntu, Red Hat, Debian, openSUSE, Amazon Linux, Oracle Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2019-5418	✗	Rails, openSUSE, Ubuntu, Red Hat, Debian	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:rubyonrails:rails:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:a:redhat:-:*:*:*:*:*:*:* cpe:2.3:o:opensuse:-:*:*:*:*:*:*:*	-
Rails Ruby on Rails Path Traversal Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-22	T1190: Exploit Public-Facing Application	Rails, Ubuntu, Red Hat, Debian, openSUSE

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-42009	✗	RoundCube Version Prior to 1.6.8 and 1.5.8, Debian, Ubuntu, openSUSE	UNC1151
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:roundcube:webmail:*:*:*:*:*:*:*:*	-
RoundCube Webmail Cross-Site Scripting Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1203: Exploitation for Client Execution	RoundCube, Debian, Ubuntu, openSUSE

Vulnerability Details

#1 In July, the Linux ecosystem addressed over 2300 vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and code execution. Over 591 new vulnerabilities were discovered and patched. HiveForce lab has identified 17 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, five of these vulnerabilities are under active exploitation, which requires urgent attention and remediation.

#3 In recent cybersecurity developments, two zero-day vulnerabilities, CVE-2025-6554 and CVE-2025-6558, have come to the forefront. CVE-2025-6554 is a critical zero-day vulnerability classified as a type confusion flaw. This issue enables attackers to corrupt memory and execute arbitrary code within the browser's context, potentially resulting in a complete browser compromise. Successful exploitation could facilitate a sandbox escape and allow remote code execution (RCE) on the host system.

#4 Another zero-day vulnerability, CVE-2025-6558, is currently being exploited in the wild, posing an immediate risk to users. The vulnerability arises from insufficient input validation within Chrome's graphics processing components. Exploitation could result in a full security bypass, giving attackers code execution capabilities outside of Chrome's secure environment.

#5 CVE-2024-38475 affects SonicWall SMA devices and is linked to improper output handling in the mod_rewrite module of Apache HTTP Server (version 2.4.59 and earlier), which these devices utilize. By exploiting this flaw, attackers can manipulate URLs to access unintended file paths on the system. In certain cases, this may lead to unauthorized file access and potential session hijacking.

#6 Lastly, the threat actor group UNC1151 has attempted to exploit CVE-2024-42009, a vulnerability in Roundcube that allows the execution of malicious JavaScript code upon opening a crafted email. No user interaction beyond opening the email is required. This flaw has been actively leveraged to harvest credentials, highlighting the dangers of client-side vulnerabilities in webmail platforms.

Recommendations

Proactive Strategies:

Adopt Secure Coding Practices: Implement strict memory management protocols and avoid unsafe functions prone to type confusion, use-after-free, or buffer overflow vulnerabilities. Regularly audit code, especially in high-risk components and authentication libraries.

Conduct Regular Penetration Testing: Perform routine security assessments to identify and mitigate vulnerabilities such as path traversal or uninitialized variables, before attackers exploit them. Testing should include dynamic analysis, particularly for complex systems.

Use OS-Level Sandboxing for Risky Processes: Run exposed or untrusted processes (like SSH services and browser instances) inside isolated containers, sandboxes, or restricted VMs to contain potential exploits.

Harden Server Configurations: Implement best practices for server hardening, such as disabling unnecessary services, restricting access to sensitive directories, and enforcing strict authentication protocols. Avoid default configurations that allow file uploads without validation.

Third-Party Software and Dependency Audits: Regularly audit third-party libraries and legacy software for unpatched vulnerabilities. Replace outdated dependencies and vulnerable versions proactively.

Reactive Strategies:

Review Email Logs and Threat Indicators: Conduct a thorough analysis of email and network logs for any communication or activity related to a.mpk-krakow[.]pl, a known indicator linked to the recent Roundcube exploitation campaign. Pay particular attention to any suspicious or unsolicited messages that may have originated from or interacted with this domain, as it could suggest attempted or successful compromise.

Deploy Network Traffic Analysis for Unusual Patterns: Monitor inbound and outbound network traffic for any unusual SSH communication patterns, especially during initial attack stages. Suspicious traffic without authentication could be indicative of exploitation attempts targeting vulnerabilities.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-32023	T1078: Valid Accounts, T1204: User Execution, T1210: Exploitation for Remote Code Execution	DS0002: User Account Authentication	M1026: Privileged Account Management, M1018: User Account Management, M1017: User Training	✓ Redis, Red Hat, Alpine, Debian, Amazon Linux, Linux Oracle
CVE-2025-32462	T1068: Exploitation for Privilege Escalation	DS0009: Process Creation	M1051: Update Software, M1038: Execution Prevention	✓ Sudo, Ubuntu, Red Hat, Debian, Alpine Linux, openSUSE, Fedora
CVE-2025-32463	T1068: Exploitation for Privilege Escalation	DS0009: Process Creation	M1051: Update Software, M1038: Execution Prevention	✓ Sudo, Ubuntu, Red Hat, Debian, openSUSE, Alpine Linux
CVE-2025-38089	T1499: Network Denial of Service, T1219: Remote Discovery	DS0015: Application Log Content	M1017: User Training, M1051: Update Software	✓ Linux kernel, Red Hat, Debian, Oracle Linux ✗ Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-48384	T1195: Supply Chain Compromise, T1059: Command and Scripting Interpreter	DS0015: Application Log Content	M1051: Update Software	✓ Git, Ubuntu, Red Hat, Alpine Linux, ✗ Debian
CVE-2025-53367	T1203: Exploitation for Client Execution, T1553: Subvert Trust Controls	DS0015: Application Log Content	M1051: Update Software, M1037: Filter Network Traffic	✓ DjVuLibre, Debian, Ubuntu, Fedora
CVE-2025-6554	T1059: Command and Scripting Interpreter, T1059.007: JavaScript, T1189: Drive-by Compromise, T1068: Exploitation for Privilege Escalation	DS0017: Command Execution, DS0015: Application Log	M1047: Audit, M1040: Behavior Prevention on Endpoint	✓ Google Chrome, Microsoft Edge, Debian
CVE-2025-6558	T1497: Virtualization/Sandbox Evasion, T1189: Drive-by Compromise	DS0017: Command Execution, DS0009: Process Creation	M1050: Exploit Protection, M1051: Update Software	✓ Google Chrome, Debian, Microsoft Edge
CVE-2025-6424	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1059.007: JavaScript	DS0009: Process Creation, DS0012: Script Execution	M1050: Exploit Protection, M1051: Update Software	✓ Mozilla Firefox, Ubuntu, Red Hat, Debian, openSUSE, Amazon Linux, Oracle Linux
CVE-2025-23048	T1190: Exploit Public-Facing Application	DS0015: Application Log	M1030: Network Segmentation, M1026: Privileged Account Management, M1051: Update Software, M1016: Vulnerability Scanning	✓ Apache, Ubuntu, Debian, ✗ Red Hat
CVE-2025-6427	T1189: Drive-by Compromise, T1210: Exploitation of Remote Services	DS0015: Application Log	M1051: Update Software	✓ Mozilla Firefox, openSUSE, Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-38001	T1068: Exploitation for Privilege Escalation, T1543: Create or Modify System Process	DS0019: Service Modification, DS0009: Process Creation	M1051: Update Software	✓ Linux Kernel, Ubuntu, Red Hat, Debian, Oracle Linux, Amazon Linux, openSUSE
CVE-2025-48988	T1499: Endpoint Denial of Service, T1496: Resource Hijacking	DS0029: Network Traffic Flow, DS0013: Sensor Health, DS0015: Application Log	M1037: Filter Network Traffic	✓ Apache Tomcat, Debian, Amazon Linux, openSUSE, ✗ Red Hat
CVE-2025-5222	T1059: Command and Scripting Interpreter	DS0017: Command Execution, DS0012: Script Execution	M1047: Audit	✓ openSUSE, Debian, Amazon Linux, ✗ Ubuntu, Red Hat
CVE-2024-38475	T1190: Exploit Public-Facing, Application; T1059: Command and Scripting Interpreter	DS0029: Network Traffic, DS0017: Command Execution	M1030: Network Segmentation, M1051: Update Software, M1016: Vulnerability Scanning	✓ Apache, Ubuntu, Red Hat, Debian, openSUSE, Amazon Linux, Oracle Linux
CVE-2019-5418	T1190: Exploit Public-Facing Application	DS0029: Network Traffic	M1050: Exploit Protection, M1035: Limit Access to Resource Over Network, M1030: Network Segmentation, M1051: Update Software	✓ Rails, Ubuntu, Red Hat, Debian, openSUSE
CVE-2024-42009	T1203: Exploitation for Client Execution	DS0009: Process Creation, DS0015: Application Log	M1050: Exploit Protection, M1051: Update Software	✓ RoundCube, Debian, Ubuntu, openSUSE

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://www.exploit-db.com/exploits/52354

https://www.exploit-db.com/exploits/52352

https://github.com/keymaker-arch/NFSundown/blob/main/poc.py

https://www.exploit-db.com/exploits/46585

https://cert.pl/en/posts/2025/06/unc1151-campaign-roundcube/

https://hivepro.com/threat-advisory/cve-2025-6554-google-chromes-zero-day-flaw-exploited-in-the-wild/

https://hivepro.com/threat-advisory/cve-2025-6558-chrome-flaw-lets-hackers-break-the-sandbox/

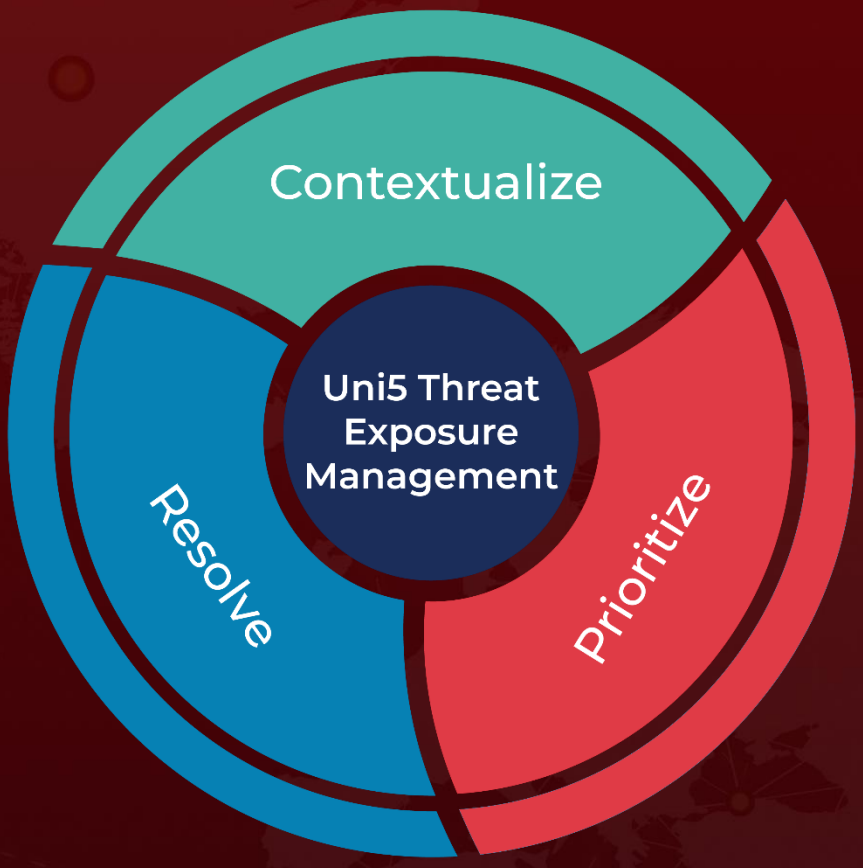
https://hivepro.com/threat-advisory/urgent-patch-required-active-attacks-exploiting-sonicwall-sma-vulnerabilities/

https://hivepro.com/threat-digest/cisa-known-exploited-vulnerability-catalog-june-2025/

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

July 25, 2025 • 9:30 AM

More at www.hivepro.com