Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

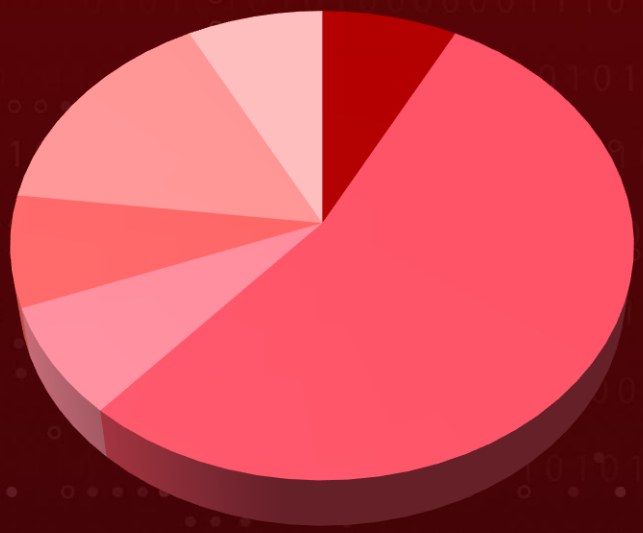
June 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
June 25, 2026	A1	TA2026177

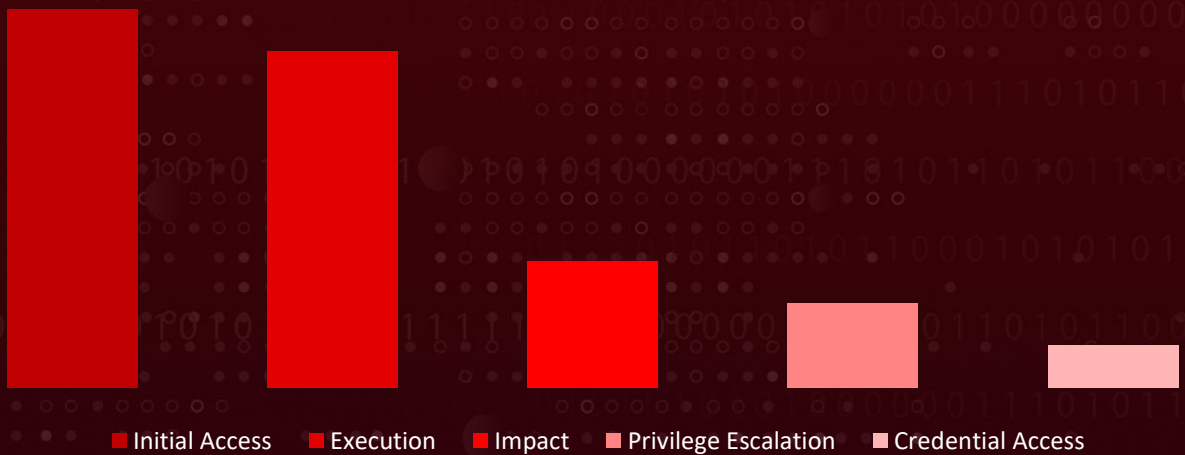
Summary

In June, more than **2416** new vulnerabilities were discovered and addressed within the Linux ecosystem, impacting several major distributions such as Debian, SUSE, Ubuntu, and Red Hat. During this period, over **2913** 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 **13** 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-2024-4741	Openssl Use-After-Free Vulnerability	OpenSSL, Ubuntu, RedHat, Debian, SUSE, Amazon Linux, Oracle	Code Execution	Network
CVE-2025-52999	Jackson-core Stack Overflow Vulnerability	Jackson-core, Red Hat, Oracle Linux, Debian, SUSE	Denial of Service	Network
CVE-2025-69720	GNU ncurses analyze_string Buffer Overflow Vulnerability	ncurses 6.4 and 6.5 (before 6.5-20251213); Red Hat, Oracle Linux, Debian, Ubuntu, SUSE	Code Execution	Local
CVE-2026-11645*	Google Chrome V8 Out-of-Bounds Read and Write Vulnerability	Google Chrome prior to 149.0.7827.103	Code Execution	Network
CVE-2024-12084	Rsync Heap-based Buffer Overflow Vulnerability	Rsync 3.2.7 through 3.3.0 (fixed in 3.4.0); Ubuntu, Debian, RedHat, SUSE, Amazon Linux, Oracle	Code Execution	Network
CVE-2024-12085	Rsync Information Disclosure Vulnerability	Rsync before 3.4.0; RedHat, Oracle Linux, Debian, Ubuntu, SUSE	Information Disclosure	Network
CVE-2026-23479	Redis Use-After-Free Vulnerability	Redis 7.2.0 through 8.6.2; Debian, SUSE, Oracle Linux, RedHat	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-2026-31402	Linux Kernel nfsd Heap-based Buffer Overflow Vulnerability	Linux Kernel (nfsd NFSv4.0); RedHat, Oracle Linux, Ubuntu, SUSE, Debian, Amazon Linux	Code Execution	Network
CVE-2026-34444	Lupa Sandbox Escape Authorization Bypass Vulnerability	Lupa (Python/PyPI) 2.6 and earlier, RedHat, Oracle Linux, SUSE, Debian	Arbitrary Code Execution	Network
CVE-2026-43512	Apache Tomcat DIGEST Authentication Bypass Vulnerability	Apache Tomcat 8.5.x, 9.0.x ≤ 9.0.117, 10.1.x ≤ 10.1.54, 11.0.x ≤ 11.0.21 (fixed in 9.0.118 / 10.1.55 / 11.0.22); Debian, SUSE, RedHat, Mageia	Unauthorized Access	Network
CVE-2026-4800	Lodash Template Code Injection Vulnerability	Lodash (npm) before 4.18.0; RedHat, Ubuntu, Debian, SUSE, Oracle	Code Execution	Network
CVE-2026-46300	Fragnesia (Linux Kernel XFRM ESP-in-TCP Page-Cache Corruption Local Privilege Escalation Vulnerability)	Linux Kernel; RedHat, Ubuntu, Debian, SUSE, Oracle, Amazon Linux	Privileged Access	Local
CVE-2026-46333	Linux Kernel ptrace "ssh-keysign-pwn" Privilege Escalation Vulnerability	Linux Kernel; RedHat, Ubuntu, Debian, SUSE, Oracle, Amazon Linux	Privileged Access	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.

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 PRODUCT	ASSOCIATED ACTORS
CVE-2026-11645	✗	Google Chrome (Before 149.0.7827.103)	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:google:chrome:*:*:*:*:*:*:*:*	-
Google Chromium V8 Out-of-Bounds Read and Write Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-125, CWE-787	T1203: Exploitation for Client Execution, T1189: Drive-by Compromise	https://www.google.com/intl/en/chrome/?standalone=1

Vulnerability Details

#1

In June, the Linux ecosystem addressed over **2913** vulnerabilities across various distributions and products, covering critical issues such as denial of service, privilege escalation, and remote code execution. HiveForce Lab has identified **13** critical vulnerabilities that are either currently being exploited or highly likely to be targeted soon. Notably, one of the vulnerabilities is under active exploitation, requiring immediate attention and remediation.

#2

The most urgent threat is browser-based. CVE-2026-11645, a high-severity out-of-bounds read and write flaw (CVSS 8.8) in V8, the JavaScript and WebAssembly engine, allows a remote attacker to execute arbitrary code inside the browser sandbox via a crafted HTML page, affecting Chrome prior to 149.0.7827.103 and all Chromium-based browsers including Edge, Brave, Opera, and Vivaldi. It is the fifth actively exploited Chrome zero-day of 2026, with an exploit confirmed in the wild and a fix shipped on June 8, 2026. This is the single vulnerability in this set requiring emergency remediation.

#3

Network-facing services present the highest remote-code-execution risk after the browser. CVE-2024-12084, a heap-based buffer overflow in the Rsync daemon (CVSS 9.8), allows an unauthenticated client to corrupt heap memory through an attacker-controlled checksum length and achieve remote code execution, and it pairs with CVE-2024-12085 (CVSS 7.5), an uninitialized-stack information disclosure flaw that leaks memory to defeat ASLR and make the overflow reliably exploitable; both are resolved in rsync 3.4.0.

#4

CVE-2026-23479, a use-after-free in the Redis unblock-client path, enables code execution as the Redis daemon for an authenticated user with sufficient privileges. CVE-2026-31402, a heap-based buffer overflow in the kernel's NFSv4.0 LOCK replay cache, can be triggered remotely by an unauthenticated attacker using two cooperating NFS clients, most plausibly causing memory corruption and service crash.

#5

Linux kernel and local privilege escalation remain prime targets. CVE-2026-46300, named "Fragnesia," is a local privilege escalation flaw in the kernel's XFRM ESP-in-TCP subsystem (CVSS 7.8); a public proof-of-concept reliably grants root on default installations by modifying a privileged binary such as /usr/bin/su in the page cache, with no race condition required.

#6

CVE-2026-46333, "ssh-keysign-pwn," abuses a missing check in __ptrace_may_access combined with the process-exit window; though scored 5.5 as information disclosure, public exploits demonstrate full local root and theft of sensitive files including OpenSSH host private keys and /etc/shadow. CVE-2025-69720, a stack-based buffer overflow in the ncurses infocmp utility, allows local code execution or crash when processing an untrusted terminfo entry.

#7

Critical flaws in widely deployed application libraries and middleware were also addressed, with real-world impact often gated by configuration. CVE-2026-34444, a sandbox-escape flaw in the Lupa Python-to-Lua bridge (CVSS 10.0), bypasses the attribute filter through built-in functions to reach arbitrary code execution in deployments that execute untrusted Lua with built-ins exposed. CVE-2026-43512, an Apache Tomcat DIGEST authentication bypass (CVSS 9.8, vendor-rated moderate), lets an attacker authenticate as any user where DIGEST authentication is enabled.

#8

CVE-2026-4800, a code-injection flaw in the Lodash template function, executes attacker JavaScript when untrusted input reaches template imports. CVE-2025-52999, a stack-overflow flaw in jackson-core (CVSS 8.7), crashes services through deeply nested JSON, and CVE-2024-4741, a low-severity use-after-free in OpenSSL's SSL_free_buffers, affects only the narrow set of applications calling that function directly.

#9

June 2026's vulnerability landscape reflects continued high-risk trends, with active exploitation of browser engines, publicly weaponized kernel privilege-escalation flaws, and remote code execution in network services and application dependencies posing the most urgent threats. Timely patching, strict configuration hardening, and defense-in-depth strategies remain essential to prevent system compromise.

Recommendations

Proactive Strategies:

Exposure Assessment: Conduct a comprehensive service exposure evaluation to identify any publicly accessible services, data-processing endpoints, or multi-tenant hosts that may be vulnerable to exploitation. Prioritize exposure assessment for internet-facing rsync daemons, Redis instances, NFSv4.0 servers, Apache Tomcat deployments using DIGEST authentication, and shared Linux hosts, CI runners, and containers where untrusted users can obtain a shell.

Regular Patch Management & Kernel Updates: Ensure all Linux distributions, installed packages, and kernel versions are updated to the latest security patches. Automate updates using tools such as unattended-upgrades, DNF Automatic, or apt-cron to reduce the window of exposure. Pay particular attention to the actively exploited CVE-2026-11645, the Rsync fixes CVE-2024-12084 and CVE-2024-12085 (rsync 3.4.0), and the kernel privilege-escalation flaws CVE-2026-46300 and CVE-2026-46333.

Reduce Attack Surface & Harden Configurations: With CVE-2024-12084 enabling unauthenticated RCE, restrict Rsync daemons to trusted networks and require authentication. Keep Redis off the public internet, enforce strong ACLs so no single role holds admin, config, and scripting privileges together, and disable scripting where Lua is unused to break CVE-2026-23479. Limit NFSv4.0 to trusted clients for CVE-2026-31402. Where kernel patching lags, apply the module blacklist for esp4/esp6/rxrpc to mitigate Fragnesia, and set kernel.yama.ptrace_scope=2 against CVE-2026-46333.

Harden Browser and Application Dependencies: With CVE-2026-11645 actively exploited in Chromium, update all browsers and email clients to the latest supported versions immediately. Audit application dependencies for vulnerable libraries, upgrading jackson-core, Lodash, Lupa, and disable DIGEST authentication on Tomcat unless explicitly required.

Reactive Strategies:

Deploy or tighten endpoint detection and response (EDR), SIEM rules, and network traffic analysis to detect exploitation attempts and persistence mechanisms. Focus on anomalous Rsync daemon connections, suspicious ptrace-based and namespace-driven kernel privilege escalation activity, page-cache tampering of privileged binaries, and browser-related script execution anomalies.

In case of system compromise, immediately isolate the host from the network to prevent further spread. Use iptables or nftables to block malicious traffic, revoke credentials of affected users and rotate exposed keys, and restore from a clean, verified backup before reconnecting.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-4741	T1190: Exploit Public-Facing Application T1203: Exploitation for Client Execution	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1051: Update Software M1050: Exploit Protection M1037: Filter Network Traffic	OpenSSL Debian Ubuntu Red Hat SUSE Oracle
CVE-2025-52999	T1190: Exploit Public-Facing Application T1499: Endpoint Denial of Service	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms	M1051: Update Software M1038: Execution Prevention M1037: Filter Network Traffic	jackson-core Red Hat Oracle Debian SUSE
CVE-2025-69720	T1204: User Execution T1499: Endpoint Denial of Service	DET0478: User Execution – multi-surface behavior chain (documents/links → helper/unpacker → LOLBIN/child → egress) DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms	M1051: Update Software M1017: User Training M1038: Execution Prevention	ncurses Red Hat Oracle Debian Ubuntu SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-11645*	T1203: Exploitation for Client Execution, T1189: Drive-by Compromise	DET0176: Drive-by Compromise — Behavior-based, Multi-platform Detection Strategy (T1189) DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1051: Update Software M1021: Restrict Web-Based Content M1050: Exploit Protection M1017: User Training	Google Chrome
CVE-2024-12084	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software M1050: Exploit Protection M1037: Filter Network Traffic	rsync Ubuntu Debian Red Hat SUSE Oracle
CVE-2024-12085	T1190: Exploit Public-Facing Application T1203: Exploitation for Client Execution	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps)	M1051: Update Software M1050: Exploit Protection M1037: Filter Network Traffic	Rsync Red Hat Oracle Debian Ubuntu SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-23479	T1190: Exploit Public-Facing Application T1059: Command and Scripting Interpreter	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software M1026: Privileged Account Management M1042: Disable or Remove Feature or Program M1037: Filter Network Traffic	Redis Debian SUSE Red Hat
CVE-2026-31402	T1190: Exploit Public-Facing Application T1499: Endpoint Denial of Service	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0208: Endpoint Resource Saturation and Crash Pattern Detection Across Platforms	M1051: Update Software M1037: Filter Network Traffic M1042: Disable or Remove Feature or Program	Linux Kernel Red Hat Oracle Ubuntu SUSE Debian
CVE-2026-34444	T1203: Exploitation for Client Execution T1059.006: Command & Scripting Interpreter: Python	DET0287: Exploitation for Client Execution – cross-platform behavior chain (browser/Office/3rd-party apps) DET0063: Cross-Platform Behavioral Detection of Python Execution	M1051: Update Software M1048: Application Isolation and Sandboxing M1038: Execution Prevention	Lupa (PyPI) Ubuntu SUSE Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-43512	T1190: Exploit Public-Facing Application T1078: Valid Accounts	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress)	M1051: Update Software M1042: Disable or Remove Feature or Program M1026: Privileged Account Management	✓ Apache Tomcat Debian SUSE Red Hat
CVE-2026-4800	T1190: Exploit Public-Facing Application T1059.007: Command & Scripting Interpreter: JavaScript	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress) DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software M1038: Execution Prevention M1048: Application Isolation and Sandboxing	✓ Lodash (npm) Red Hat Ubuntu SUSE Oracle ✗ Debian
CVE-2026-46300	T1068: Exploitation for Privilege Escalation T1611: Escape to Host	DET0514: Detection Strategy for Exploitation for Privilege Escalation	M1051: Update Software M1038: Execution Prevention M1042: Disable or Remove Feature or Program	✓ Linux Kernel Red Hat SUSE Oracle ✗ Ubuntu Debian

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2026-46333	T1068: Exploitation for Privilege Escalation T1003.008: OS Credential Dumping T1552.004: Unsecured Credentials: Private Keys	DET0514: Detection Strategy for Exploitation for Privilege Escalation DET0446: Credential Access via /etc/passwd and /etc/shadow Parsing DET0549: Detect Suspicious Access to Private Key Files and Export Attempts Across Platforms	M1051: Update Software M1028: Operating System Configuration M1038: Execution Prevention	✓ Linux Kernel Red Hat Ubuntu SUSE Oracle ✗ Debian

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.hivepro.com/threat-advisory/google-rushes-patch-for-in-the-wild-chrome-v8-zero-day-cve-2026-11645

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 Demo of **HivePro**.

REPORT GENERATED ON

June 25, 2026 • 09:30 AM

More at www.hivepro.com