Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

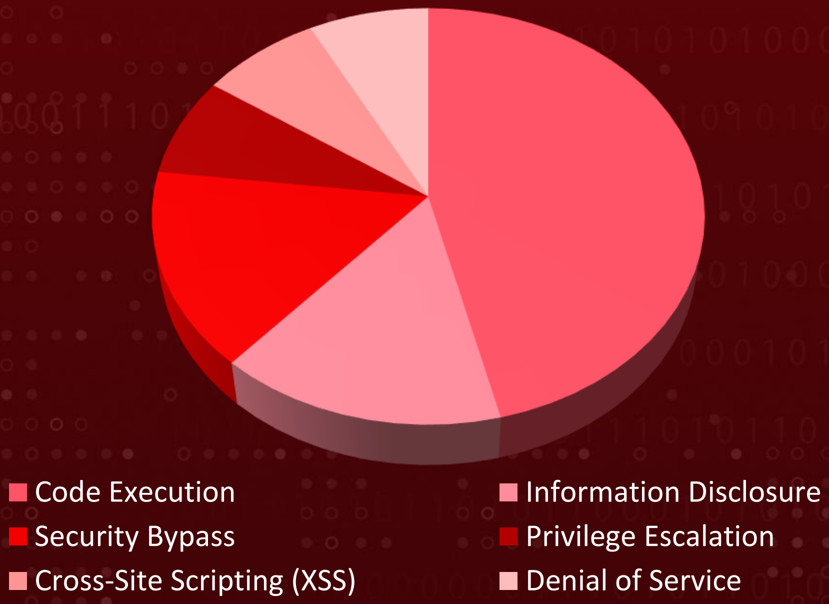
April 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
April 24, 2025	A1	TA2025126

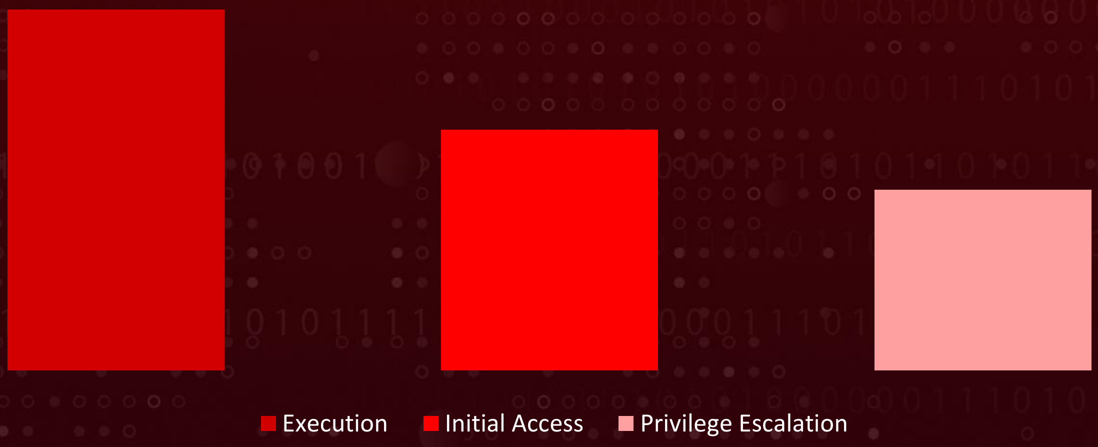
Summary

In April, more than **591** 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 **2400** 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 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-2025-32433*	Erlang/OTP Unauthenticated Remote Code Execution Vulnerability	Erlang/OTP, Ubuntu, Debian, SUSE	Unauthorized Access	Remote
CVE-2024-6827	Gunicorn HTTP Request Smuggling Vulnerability	Gunicorn version 21.2.0, Debian, Wolfi, RedHat, SUSE	Data Exposure	Network
CVE-2025-2476	Chrome Use-after-free in Lens Vulnerability	Chrome prior to 134.0.6998.117, Debian, SUSE	Code Execution	Network
CVE-2025-1219	PHP Validation Bypass Vulnerability	PHP, Amazon Linux, SUSE, RedHat, Debian, Ubuntu	Data Integrity	Network
CVE-2024-50302*	Linux Kernel Use of Uninitialized Resource Vulnerability	Linux Kernel, Red Hat Enterprise Linux CoreOS (RHCOS), Debian, Ubuntu, SUSE, Amazon Linux, Oracle Linux	Information Disclosure	Local
CVE-2022-0995	Linux Kernel Watch_Queue Out-of-Bounds Write Vulnerability	Linux Kernel, Debian, Ubuntu, SUSE, Linux Photon	Privileged Access	Local
CVE-2024-4741	Openssl Use-After-Free Vulnerability	OpenSSL, Ubuntu, RedHat, Debian, SUSE, Amazon Linux, Oracle	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-2024-53197*	Linux Kernel Out-of-Bounds Access Vulnerability	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	Privilege Escalation	Local
CVE-2024-53150*	Linux Kernel Out-of-Bounds Read Vulnerability	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	Information Disclosure	Local
CVE-2020-11023*	JQuery Cross-Site Scripting (XSS) Vulnerability	JQuery, Rocky Linux, Debian, Ubuntu, RedHat, SUSE, Amazon Linux, CentOS, Oracle Linux	Code Execution	Network
CVE-2023-45288	Golang HTTP/2 CONTINUATION Flood Vulnerability	Golang, Rocky Linux, Debian, Ubuntu, RedHat, SUSE, Amazon Linux, Oracle Linux	Denial of Service	Network
CVE-2025-30472	Corosync Stack-Based Buffer Overflow Vulnerability	Corosync, Debian, Fedora, RedHat, SUSE	Code Execution	Network
CVE-2025-29482	libheif Buffer Overflow Vulnerability	libheif, Debian, Ubuntu	Code Execution	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-2025-32433	☒	All Erlang/OTP SSH servers running versions: OTP-27.3.2 and earlier OTP-26.2.5.10 and earlier OTP-25.3.2.19 and earlier	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:erlang:otp:*:*:*:*:*:*:*:*	-
	☒		
Erlang/OTP Unauthenticated Remote Code Execution Vulnerability	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-306	T1059: Command and Scripting Interpréter; T1059.004: Unix Shell; T1059.006: Python; T1133: External Remote Services; T1190: Exploit Public-Facing Application	Erlang/OTP, Ubuntu, Debian, SUSE

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-50302	✗	Linux Kernels before 5.4.286, Kernels before 4.19.324, Kernels before 5.10.230, Kernels before 5.15.172, Kernels before 6.1.117, Kernels before 6.6.61, Kernels before 6.11.8	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	NoviSpy
Linux Kernel Use of Uninitialized Resource Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-908	T1499: Endpoint Denial of Service; T1574: Hijack Execution Flow	Linux Kernel, Red Hat Enterprise Linux CoreOS (RHCOS), Debian, Ubuntu, SUSE, Amazon Linux, Oracle Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53197	✗	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	-
	ZERO-DAY		
	✓	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Access Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-787	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2024-53150	✗	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux	-
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:o:linux:linux_kernel:*:*:*:*:*:*:*:*	-
Linux Kernel Out-of-Bounds Read Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-125	T1068: Exploitation for Privilege Escalation; T1574: Hijack Execution Flow	Linux Kernel, Debian, Ubuntu, RedHat, SUSE, Oracle Linux

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2020-11023	✗	jQuery versions greater than or equal to 1.0.3 and before 3.5.0	APT1, APT27
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*	-
JQuery Cross-Site Scripting (XSS) Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-79	T1189: Drive-By Compromise; T1204.001: Malicious Link; T1204: User Execution	Jquery, Rocky Linux, Debian, Ubuntu, RedHat, SUSE, Amazon Linux, CentOS, Oracle Linux

Vulnerability Details

#1 In April, the Linux ecosystem addressed over 2400 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 13 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-2024-50302 and CVE-2024-53197, have come to the forefront. The state-sponsored espionage groups have allegedly exploited CVE-2024-50302, a flaw employing Cellebrite's mobile forensic tools, to infiltrate Android devices belonging to student activists in Serbia. This alarming revelation underscores the persistent targeting of civil society through sophisticated surveillance techniques.

#4 Meanwhile, CVE-2024-53197 has been identified as a privilege escalation vulnerability within the USB audio sub-system of the Linux Kernel. This flaw enables local attackers to access sensitive information on affected devices without requiring any user interaction, posing a significant threat to system integrity and privacy.

#5 Adding to the list of concerning disclosures is a five-year-old jQuery cross-site scripting (XSS) vulnerability, CVE-2020-11023. Despite being publicly disclosed back in April 2020, this medium-severity flaw remains actively exploited. Notorious APT groups such as APT1 (also known as Brown Fox or Comment Panda) and APT27 (dubbed Brown Worm or Emissary Panda) have reportedly leveraged this vulnerability for arbitrary code execution in targeted campaigns.

#6 More recently, CVE-2025-32433, a critical vulnerability affecting the SSH server component of the Erlang/OTP programming platform, has emerged. This flaw allows a remote attacker to execute arbitrary code on a vulnerable system without authentication. By sending specially crafted SSH messages, an attacker could seize complete control of a server without needing a username or password, making this vulnerability particularly dangerous in exposed infrastructure.

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 like vulnerable jQuery versions proactively.

Reactive Strategies:

Analyze Endpoint Behavior for Anomalies: Monitor for unusual memory or process behavior indicative of privilege escalation attempts, such as suspicious kernel-level access or abnormal device interactions. EDR solutions can detect these irregularities in real-time.

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 like CVE-2025-32433.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-32433	T1059: Command and Scripting Interpreter T1059.004: Unix Shell T1059.006: Python T1133: External Remote Services T1190: Exploit Public-Facing Application	DS0017: Command DS0009: Process DS0028: Logon Session DS0029: Network Traffic	M1021: Restrict Web-Based Content M1040: Behavior Prevention on Endpoint M1030: Network Segmentation M1050: Exploit Protection	✓ Erlang/OTP Ubuntu Debian SUSE
CVE-2024-6827	T1190: Exploit Public-Facing Application T1505: Server Software Component T1071: Application Layer Protocol	DS0029: Network Traffic DS0015: Application Log DS0017: Command	M1030: Network Segmentation M1050: Exploit Protection M1037: Filter Network Traffic	✓ Gunicorn Debian Wolfi RedHat SUSE
CVE-2025-2476	T1189: Drive-By Compromise	DS0029: Network Traffic DS0015: Application Log	M1051: Update Software M1026: Privileged Account Management M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ Chrome Debian SUSE
CVE-2025-1219	T1190: Exploit Public-Facing Application T1040: Network Sniffing	DS0029: Network Traffic DS0017: Command	M1050: Exploit Protection M1026: Privileged Account Management M1030: Network Segmentation M1016: Vulnerability Scanning	✓ PHP Amazon Linux SUSE RedHat Debian Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-50302	T1499: Endpoint Denial of Service T1574: Hijack Execution Flow	DS0029: Network Traffic DS0015: Application Log	M1037: Filter Network Traffic	✓ Linux Kernel Red Hat Enterprise Linux CoreOS (RHCOS) Debian Ubuntu SUSE Amazon Linux Oracle Linux
CVE-2022-0995	T1499: Endpoint Denial of Service T1068: Exploitation for Privilege Escalation	DS0029: Network Traffic DS0009: Process	M1037: Filter Network Traffic M1051: Update Software	✓ Linux Kernel Debian Ubuntu SUSE Linux Photon
CVE-2024-4741	T1189: Drive-By Compromise	DS0029: Network Traffic DS0015: Application Log	M1051: Update Software M1026: Privileged Account Management M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1021: Restrict Web-Based Content M1017: User Training	✓ OpenSSL Ubuntu RedHat Debian SUSE Amazon Linux Oracle Linux
CVE-2024-53197	T1068: Exploitation for Privilege Escalation T1574: Hijack Execution Flow	DS0017: Command DS0009: Process	M1038: Execution Prevention M1050: Exploit Protection	✓ Linux Kernel Debian Ubuntu RedHat SUSE Oracle Linux
CVE-2024-53150	T1068: Exploitation for Privilege Escalation T1574: Hijack Execution Flow	DS0017: Command DS0009: Process	M1038: Execution Prevention M1050: Exploit Protection	✓ Linux Kernel Debian Ubuntu RedHat SUSE Oracle Linux

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2020-11023	T1189: Drive-By Compromise T1204.001: Malicious Link T1204: User Execution	DS0029: Network Traffic DS0015: Application Log DS0017: Command	M1021: Restrict Web-Based Content M1050: Exploit Protection	✓ Jquery Rocky Linux Debian Ubuntu RedHat SUSE Amazon Linux CentOS Oracle Linux
CVE-2023-45288	T1071.001: Web Protocols	DS0029: Network Traffic	M1031: Network Intrusion Prevention	✓ Golang Rocky Linux Debian Ubuntu RedHat SUSE Amazon Linux Oracle Linux
CVE-2025-30472	T1574: Hijack Execution Flow T1499.004: Application or System Exploitation	DS0017: Command DS0029: Network Traffic	M1051: Update Software M1038: Execution Prevention M1037: Filter Network Traffic	✓ Corosync Debian Fedora RedHat SUSE
CVE-2025-29482	T1574: Hijack Execution Flow T1499.004: Application or System Exploitation	DS0017: Command DS0029: Network Traffic	M1051: Update Software M1038: Execution Prevention M1037: Filter Network Traffic	✓ libheif Debian Ubuntu

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/

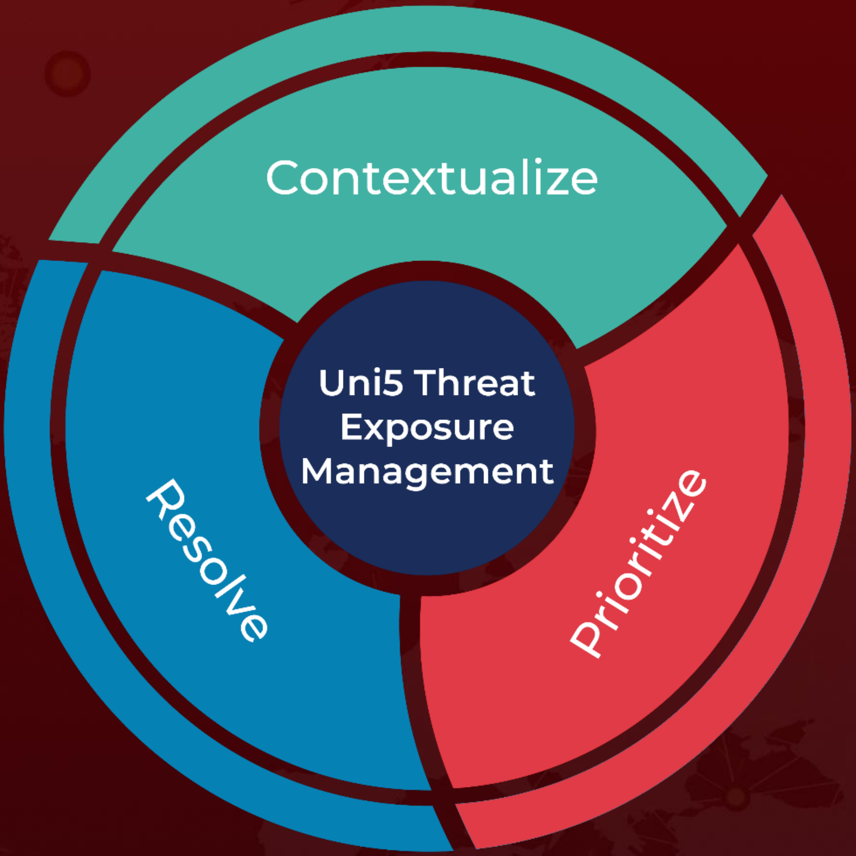
https://access.redhat.com/security/security-updates/

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 24, 2025 • 10:30 PM

More at www.hivepro.com