Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

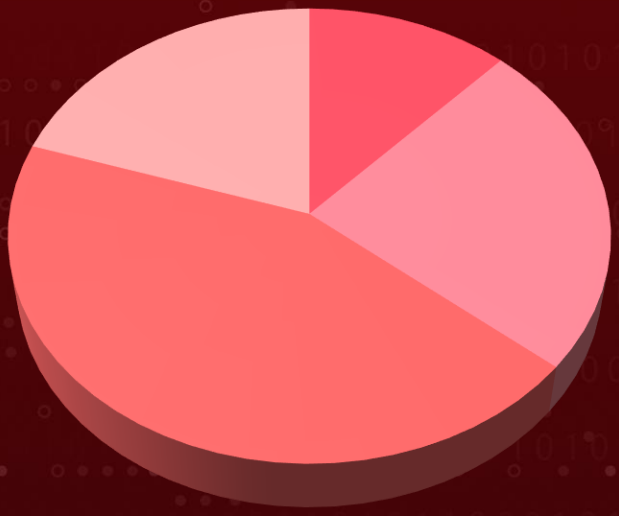
April 2026 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
April 23, 2026	A1	TA2026111

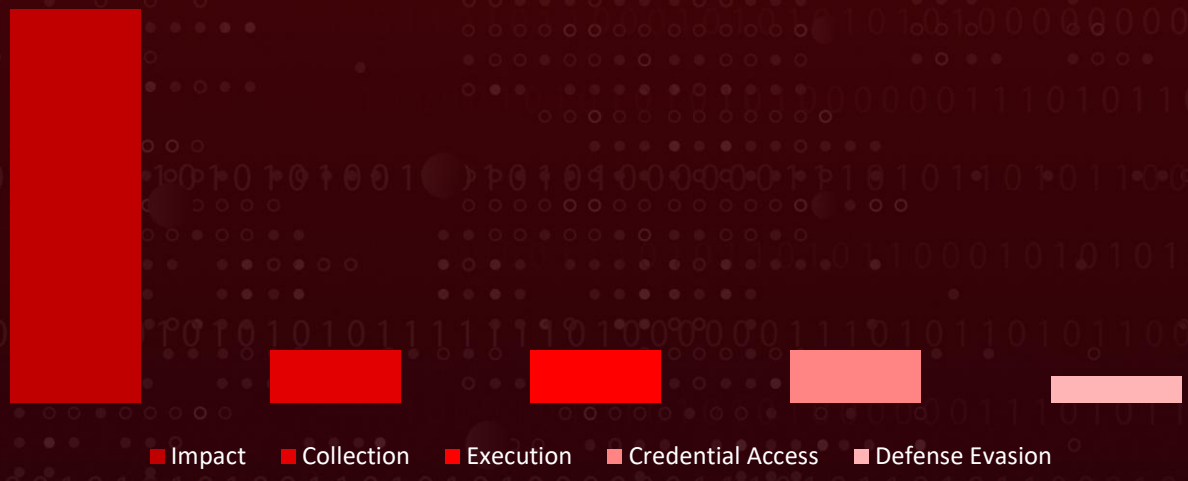
Summary

In April, more than **1105** 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 **1555** 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 22 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-2020-13935	Apache Tomcat WebSocket Payload Length Denial of Service Vulnerability	Debian, Ubuntu, SUSE	Execution	Network
CVE-2020-17527	Apache Tomcat HTTP/2 Request Header Mix-up Information Disclosure Vulnerability	Debian, Ubuntu, SUSE	Collection	Network
CVE-2024-21733	Apache Tomcat Error Message Sensitive Information Disclosure Vulnerability	Debian, Ubuntu, SUSE	Collection	Network
CVE-2025-14847*	MongoBleed (MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability)	Ubuntu, Debian, MongoDB	Credential Access	Network
CVE-2025-31277*	Apple Multiple Products Buffer Overflow Vulnerability	Debian, SUSE, Ubuntu	Execution	Network
CVE-2025-38109	Linux Kernel net/mlx5 ECVF Vports Unload Use-After-Free Vulnerability	RedHat, Debian, Ubuntu	Execution	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-2025-40153	Linux Kernel mm/hugetlb mprotect Soft Lockup Vulnerability	Debian, SUSE, RedHat, Ubuntu	Collection	Local
CVE-2025-40170	Linux Kernel Socket sk_setup_caps RCU Race Condition Vulnerability	SUSE, RedHat, Debian, Ubuntu	Execution	Local
CVE-2025-61912	Python-LDAP escape_dn_chars NUL Byte Client-Side Denial of Service Vulnerability	Ubuntu, Debian, SUSE	Execution	Network
CVE-2025-67726	Python Tornado HTTP Header Parameter Parsing Quadratic Complexity Denial of Service Vulnerability	Debian, Ubuntu, SUSE	Execution	Network
CVE-2025-68183	Linux Kernel IMA_DIGSIG Flag Clearing on xattr Modification Vulnerability	Debian, Ubuntu, RedHat, SUSE	Defense Evasion	Local
CVE-2025-68330	Linux Kernel BMC150 Accelerometer IRQ NULL Pointer Dereference Vulnerability	Debian, Ubuntu, SUSE	Collection	Local
CVE-2025-68752	Linux Kernel iavf PTP Clock settime64 NULL Pointer Dereference Vulnerability	Ubuntu, RedHat, SUSE	Discovery	Local
CVE-2025-68776	Linux Kernel net/hsr prp_get_untagged_frame NULL Pointer Dereference Vulnerability	Ubuntu, Debian, SUSE	Discovery	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-2025-68791	Linux Kernel FUSE-over-io_uring Argument Copy Reference Count Leak Vulnerability	Ubuntu, Debian, SUSE	Collection	Local
CVE-2025-69228	AIOHTTP Request.post() Uncontrolled Memory Allocation Denial of Service Vulnerability	Debian, Ubuntu, SUSE	Execution	Network
CVE-2025-69648	GNU Binutils readelf DWARF .debug_rnglists Infinite Loop Denial of Service Vulnerability	Debian, Ubuntu, RedHat, SUSE	Execution	Local
CVE-2025-69720	GNU ncurses analyze_string Buffer Overflow Vulnerability	Debian, Ubuntu, RedHat, SUSE	Execution	Local
CVE-2025-71078	Linux Kernel PowerPC Hash MMU SLB Multi-hit Vulnerability	Debian, Ubuntu, SUSE, RedHat	Collection	Local
CVE-2025-71085	Linux Kernel IPv6 CALIPSO pskb_expand_head Integer Overflow Vulnerability	Debian, Ubuntu, SUSE, RedHat	Execution	Local
CVE-2025-71108	Linux Kernel USB Type-C UCSI num_connectors Reserved-Bit Handling Vulnerability	Debian, Ubuntu, SUSE	Execution	Local
CVE-2026-33634*	Aqua Security Trivy Supply Chain Embedded Malicious Code Injection Vulnerability	Aqua Security Trivy, Container/CI-CD Platforms	Credential Access	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.

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-2025-14847	MongoBleed	MongoDB and MongoDB Server, Ubuntu, Debian	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:mongodb:mongodb:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:*	-
MongoDB and MongoDB Server Improper Handling of Length Parameter Inconsistency Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-130	T1190: Exploit Public-Facing Application, T1005: Data from Local System, T1552: Unsecured Credentials, T1213: Data from Information Repositories	MongoDB, Ubuntu, Debian

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2025-31277	✗	Apple Multiple Products, Debian, SUSE, Ubuntu	UNC6748, UNC6353
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apple:safari:*:*:*:*:*:*:*:* cpe:2.3:o:apple:ipados:*:*:*:*:*:*:*:* cpe:2.3:o:apple:iphone_os:*:*:*:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:tvos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:visionos:*:*:*:*:*:*:*:* cpe:2.3:o:apple:watchos:*:*:*:*:*:*:*:* cpe:2.3:o:debian:debian_linux:-:*:*:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:-:*:*:*:*:*:*:* cpe:2.3:o:suse:linux:*:*:*:*:*:*:*	GHOSTBLADE GHOSTKNIFE GHOSTSABER
Apple Multiple Products Buffer Overflow Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-119	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript	Apple, Debian, SUSE, Ubuntu

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
CVE-2026-33634	✗	Aquasecurity Trivy	TeamPCP
	ZERO-DAY		
	✗	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:aquasec:setup-trivy:*:*:*:*:*:*:*:*	-
Aqua Security Trivy Supply Chain Embedded Malicious Code Injection Vulnerability	✓		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-506	T1195: Supply Chain Compromise, T1195.002: Compromise Software Supply Chain, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1552.007: Container API, T1078: Valid Accounts	Aquasecurity Trivy

Vulnerability Details

#1

In April, the Linux ecosystem addressed over **2660** vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and code execution. Over **1105** new vulnerabilities were discovered and patched. HiveForce lab has identified 22 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, four of these vulnerabilities are under active exploitation, which requires urgent attention and remediation.

#3

CVE-2025-14847 (MongoBleed) is a critical unauthenticated memory-disclosure vulnerability in MongoDB Server's zlib protocol header parser, where improper handling of length parameter inconsistencies allows a remote attacker to read uninitialized heap memory by sending malformed compressed messages, potentially exposing credentials, API keys, and session tokens resident in server memory. The flaw affects MongoDB with roughly 87,000 internet-exposed instances at the time of disclosure, and it saw rapid exploitation in the wild.

#4

Building on this theme of memory corruption in widely deployed software, CVE-2025-31277 strikes at Apple's WebKit browser engine with a buffer overflow that enables arbitrary code execution through maliciously crafted web content. It is one component of the six-vulnerability DarkSword exploit chain deployed since November 2025 by commercial spyware vendors and state-aligned actors, with downstream impact extending beyond Safari and iOS into Linux ecosystems via WebKitGTK and WPE WebKit packages shipped by Debian, Ubuntu, and SUSE.

#5

Where MongoBleed and DarkSword weaponize code defects, CVE-2026-33634 represents a fundamentally different threat class, a supply chain compromise in which threat actor TeamPCP exploited a non-atomic credential rotation window to publish malicious Trivy v0.69.4, force-push 76 of 77 'trivy-action' GitHub Action tags, and replace all 7 'setup-trivy' tags with backdoored commits on March 19, 2026, deploying an infostealer that harvested CI/CD secrets from runner memory and triggered the downstream LiteLLM PyPI compromise and forcing a broad industry reckoning on immutable commit-SHA pinning and atomic secret rotation.

#6

The remaining nineteen CVEs cluster naturally into four product families, each reflecting a distinct attack surface across Linux distributions. Three Apache Tomcat flaws (CVE-2020-13935, CVE-2020-17527, CVE-2024-21733) sit at the network-exposed Java servlet layer, covering WebSocket frame denial-of-service via infinite loop, HTTP/2 stream header mix-up leading to cross-request information disclosure, and incomplete POST error responses that leak data between users, and backported across Debian, Ubuntu, and SUSE.

#7

The largest cluster, spanning eleven Linux kernel CVEs, divides cleanly by impact: nine denial-of-service flaws (CVE-2025-38109, -40153, -40170, -68330, -68752, -68776, -68791, -71078, -71108) affect subsystems ranging from the mlx5 networking driver and hugetlb memory management to the iavf PTP clock, and USB Type-C UCSI parsing collectively enabling kernel panics, NULL-pointer dereferences, and memory exhaustion through local attack vectors.

#8

Shifting from kernel to userspace, three Python ecosystem vulnerabilities (CVE-2025-61912, CVE-2025-67726, CVE-2025-69228) expose 'python-ldap', Tornado, and AIOHTTP, respectively, to remote denial-of-service through a NUL-byte escape failure in DN construction, HTTP header parameter parsing, and uncontrolled memory allocation. Finally, two GNU toolchain flaws (CVE-2025-69648, CVE-2025-69720) target core developer utilities, with a 'readelf' infinite-loop DoS when parsing malformed DWARF data and a buffer overflow in 'ncurses' 'analyze_string()' that carries a public PoC and the potential for arbitrary code execution in any application linked against the vulnerable library, extending the remediation footprint to essentially every Debian, Ubuntu, RHEL, and SUSE system in operation.

Recommendations

Proactive Strategies:

Harden Server and Service Configurations: Apply strict configuration baselines that disable unnecessary features and default attack surfaces. Examples include omitting zlib from MongoDB's compression compressors list, restricting HTTP/2 exposure where not required on Apache Tomcat, disabling unused kernel modules and subsystems, and tightening sysfs and IIO permissions to prevent unprivileged access to vulnerable driver paths.

Enforce Network Segmentation and Least Privilege: Isolate network-facing services such as MongoDB, Tomcat, and Python web frameworks behind segmentation boundaries, firewalls, and rate-limiting controls to blunt denial-of-service amplification and unauthorized exposure. Enforce least-privilege access on administrative interfaces and database services, and restrict inbound traffic to trusted IP ranges wherever operationally feasible.

Harden the Software Supply Chain: Pin all third-party GitHub Actions and CI/CD dependencies to full immutable commit SHA hashes rather than mutable version tags, execute atomic credential rotations that invalidate all tokens simultaneously, and transition cloud authentication to OpenID Connect (OIDC) to eliminate long-lived secrets resident in runner memory. Regularly audit repositories and build artifacts for unauthorized modifications.

Validate Inputs and Restrict Untrusted Content: Enforce strict input validation on web-exposed endpoints, including bounds checks on HTTP headers, multipart parameters, and LDAP distinguished names, to reduce exposure to parsing-based denial-of-service flaws. For endpoints and workstations, restrict execution of untrusted web content through browser sandboxing, content filtering, and application isolation to contain drive-by exploitation.

Reactive Strategies:

System Isolation and Containment: Immediately isolate affected workloads, containers, or management servers to prevent further spread. In cloud environments, quarantine compromised nodes and restrict API interactions until integrity is restored.

Deploy Network Traffic Analysis for Unusual Patterns: Continuously monitor inbound and outbound network traffic to detect anomalies such as unexpected SSH connections, unusual data flows, or communication over non-standard ports. Establish behavioral baselines for normal traffic and configure alerts for deviations, as these may indicate exploitation attempts targeting vulnerabilities. Integrating NTA with SIEM/EDR platforms enhances real-time detection and rapid response.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2020-13935	T1190: Exploit Public-Facing Application, T1498: Network Denial of Service, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0498: Behavior-chain detection for T1134.003 Make and Impersonate Token	M1051: Update Software, M1030: Network Segmentation, M1037: Filter Network Traffic	Debian, Ubuntu, SUSE
CVE-2020-17527	T1190: Exploit Public-Facing Application, T1213: Data from Information Repositories, T1040: Network Sniffing	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0213: Detection Strategy for Data Transfer Size Limits and Chunked Exfiltration, DET0040: Detection of Persistence Artifact Removal Across Host Platforms	M1051: Update Software, M1030: Network Segmentation, M1041: Encrypt Sensitive Information	Debian, Ubuntu, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-21733	T1190: Exploit Public-Facing Application, T1213: Data from Information Repositories, T1078: Valid Accounts	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0213: Detection Strategy for Data Transfer Size Limits and Chunked Exfiltration	M1051: Update Software, M1041: Encrypt Sensitive Information, M1030: Network Segmentation	Debian, Ubuntu, SUSE
CVE-2025-14847*	T1190: Exploit Public-Facing Application, T1005: Data from Local System, T1552: Unsecured Credentials, T1213: Data from Information Repositories	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0005: Renamed Legitimate Utility Execution with Metadata Mismatch and Suspicious Path	M1051: Update Software, M1030: Network Segmentation, M1041: Encrypt Sensitive Information, M1054: Software Configuration	Ubuntu, Debian, MongoDB
CVE-2025-31277*	T1189: Drive-by Compromise, T1203: Exploitation for Client Execution, T1059: Command and Scripting Interpreter, T1059.007: JavaScript	DET0189: Detection Strategy for Indicator Removal from Tools - Post-AV Evasion Modification, DET0203: Detection Strategy for Ptrace-Based Process Injection on Linux, DET0516: Behavioral Detection of Command and Scripting Interpreter Abuse	M1051: Update Software, M1048: Application Isolation and Sandboxing, M1021: Restrict Web-Based Content	Apple, Debian, SUSE, Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-38109	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1068: Exploitation for Privilege Escalation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1026: Privileged Account Management, M1038: Execution Prevention	RedHat, Debian, Ubuntu
CVE-2025-40153	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1038: Execution Prevention	Debian, SUSE, RedHat, Ubuntu
CVE-2025-40170	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1068: Exploitation for Privilege Escalation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1026: Privileged Account Management	SUSE, RedHat, Debian, Ubuntu

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-61912	T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application - anomalous DN strings with embedded NUL bytes, DET0499: Behavioral Detection of Fallback or Alternate C2 Channels	M1051: Update Software, M1054: Software Configuration, M1038: Execution Prevention	Ubuntu, Debian, SUSE
CVE-2025-67726	T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0499: Behavioral Detection of Endpoint Denial of Service - Tornado event-loop stall and CPU spike correlation	M1051: Update Software, M1030: Network Segmentation, M1037: Filter Network Traffic	Debian, Ubuntu, SUSE
CVE-2025-68183	T1553: Subvert Trust Controls, T1222: File and Directory Permissions Modification, T1222.002: Linux and Mac File and Directory Permissions Modification	DET0553: Detection Strategy for Obfuscated Files or Information: Binary Padding, DET0222: Detecting MMC (.msc) Proxy Execution and Malicious COM Activation, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1022: Restrict File and Directory Permissions, M1047: Audit	Debian, Ubuntu, RedHat, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-68330	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1038: Execution Prevention, M1022: Restrict File and Directory Permissions	Debian, Ubuntu, SUSE
CVE-2025-68752	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1026: Privileged Account Management	Ubuntu, SUSE
CVE-2025-68776	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1498: Network Denial of Service	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0498: Behavior-chain detection for T1134.003 Make and Impersonate Token	M1051: Update Software, M1030: Network Segmentation	Ubuntu, Debian, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-68791	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1038: Execution Prevention	Ubuntu, Debian
CVE-2025-69228	T1190: Exploit Public-Facing Application, T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0080: Exploit Public-Facing Application – multi-signal correlation (request → error → post-exploit process/egress), DET0499: Behavioral Detection of Fallback or Alternate C2 Channels	M1051: Update Software, M1030: Network Segmentation, M1037: Filter Network Traffic	Debian, Ubuntu, SUSE
CVE-2025-69648	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1204: User Execution, T1204.002: Malicious File	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels	M1051: Update Software, M1038: Execution Prevention, M1049: Antivirus/Antimalware	Debian, Ubuntu, RedHat, SUSE
CVE-2025-69720	T1203: Exploitation for Client Execution, T1068: Exploitation for Privilege Escalation, T1204: User Execution, T1204.002: Malicious File	DET0203: Detection Strategy for Ptrace-Based Process Injection on Linux, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1038: Execution Prevention, M1048: Application Isolation and Sandboxing	Debian, Ubuntu, RedHat, SUSE

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2025-71078	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software	Debian, Ubuntu, SUSE, RedHat
CVE-2025-71085	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1068: Exploitation for Privilege Escalation	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels, DET0068: Detection Strategy for T1505.004 - Malicious IIS Components	M1051: Update Software, M1026: Privileged Account Management, M1030: Network Segmentation	Debian, Ubuntu, SUSE, RedHat
CVE-2025-71108	T1499: Endpoint Denial of Service, T1499.004: Application or System Exploitation, T1200: Hardware Additions	DET0499: Behavioral Detection of Fallback or Alternate C2 Channels	M1051: Update Software, M1035: Limit Hardware Installation	Debian, Ubuntu, SUSE
CVE-2026-33634*	T1195: Supply Chain Compromise, T1195.002: Compromise Software Supply Chain, T1552: Unsecured Credentials, T1552.001: Credentials In Files, T1552.007: Container API, T1078: Valid Accounts	DET0195: Behavioral Detection of System Network Configuration Discovery	M1051: Update Software, M1016: Vulnerability Scanning, M1022: Restrict File and Directory Permissions, M1018: User Account Management, M1026: Privileged Account Management	Aqua Security Trivy

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://hivepro.com/threat-advisory/excobalts-gored-the-silent-infiltrator-of-russian-sectors/

https://hivepro.com/threat-advisory/june-2025-linux-patch-roundup/

https://access.redhat.com/sites/default/files/attachments/cve-2019-11135--2019-11-12-1735.sh

https://access.redhat.com/articles/tsx-asynchronousabort

https://access.redhat.com/security/cve/cve-2019-19338

https://www.exploit-db.com/exploits/49766

https://www.wiz.io/blog/nvidia-ai-vulnerability-cve-2025-23266-nvidiascape

https://github.com/advisories/GHSA-8j63-96wh-wh3j

https://cdn2.qualys.com/2025/06/17/suse15-pam-udisks-lpe.txt

https://hivepro.com/threat-advisory/teampcp-automated-supply-chain-from-trivy-to-litellm-in-a-multi-ecosystem-breach/

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

April 23, 2026 • 6:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com