Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

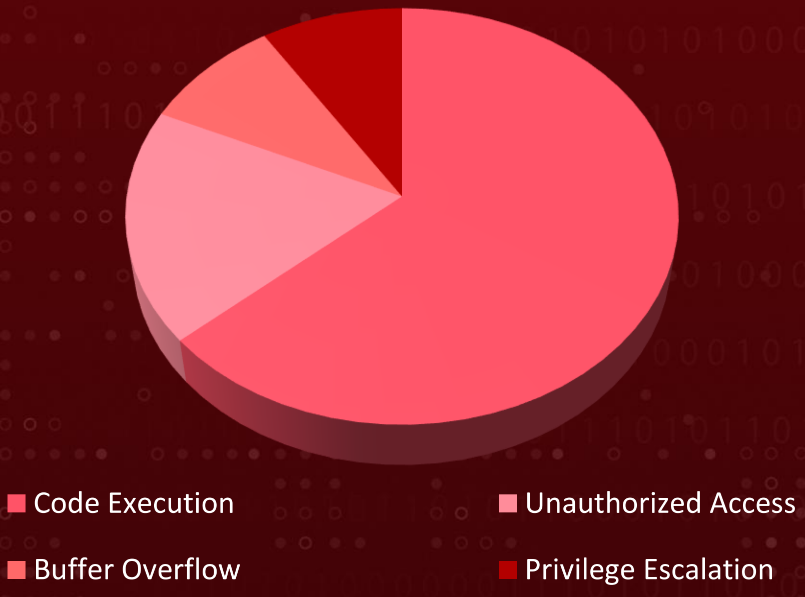
January 2025 Linux Patch Roundup

Date of Publication	Admiralty Code	TA Number
January 28, 2025	A1	TA2025022

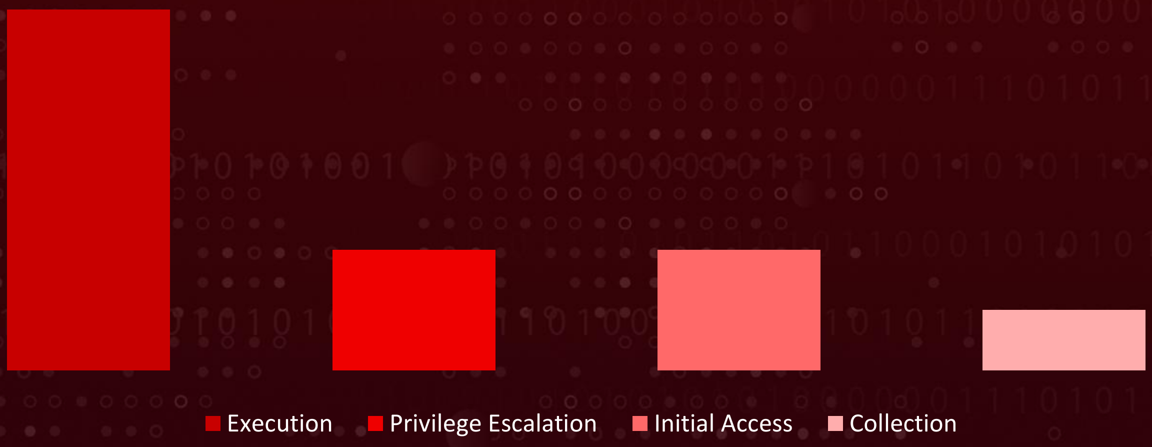
Summary

In January, more than 650 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 1000 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 11 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-2024-12381	Google Chrome Type Confusion in V8 Vulnerability	Chromium, Google Chrome	Code Execution	Phishing
CVE-2024-12692	Google Chrome Type Confusion in V8 Vulnerability	Chromium, Google Chrome	Code Execution	Phishing
CVE-2024-45337	SSH Public Key Misuse Authorization Bypass	golang-x-crypto package, Fedora, openSUSE, CBL Mariner 2.0	Unauthorized Access	Network
CVE-2024-47540	Gstreamer Arbitrary Code Execution Vulnerability	GStreamer lib, Debian, Fedora, Ubuntu, RHEL, Alma Linux, Oracle Linux, Free BSD	Arbitrary Code Execution	Network
CVE-2024-50379*	Apache Tomcat Unauthenticated Remote Code Execution Vulnerability	Apache Tomcat versions 11.0.0-M1 to 11.0.1, 10.1.0-M1 to 10.1.33, and 9.0.0.M1 to 9.0.97	Remote Code Execution	Remote
CVE-2024-12084	Rsync Heap Buffer Overflow Vulnerability	Rsync 3.2.7 or higher, and lower than 3.4.0.	Information Disclosure	Network
CVE-2024-45387	Apache Remote Code Execution Vulnerability	Apache Traffic Control 8.0.0 through 8.0.1	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-2024-56337	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat 11.0.0-M1 to 11.0.1 Apache Tomcat 10.1.0-M1 to 10.1.33 Apache Tomcat 9.0.0.M1 to 9.0.97	Remote Code Execution	Network
CVE-2025-0247	Firefox Memory Safety Vulnerability	Firefox < 134 and Thunderbird < 134.	Remote Code Execution	Network
CVE-2025-21613	Go-Git Argument Injection Vulnerability	Go-git versions: 4.0.0 (inclusive) - 5.13.0 (excluded)	Code Execution	Local
CVE-2024-54534	WebKitGTK Memory Corruption Vulnerability	libwebkit2gtk3, RHEL, SUSE Linux Enterprise Server, Apple Multiple Products including macOS, libjavascriptcoregtk, typelib-1_0	Data Corruption	Phishing

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-2024-50379*	☒	Apache Tomcat versions 11.0.0-M1 to 11.0.1, 10.1.0-M1 to 10.1.33, and 9.0.0.M1 to 9.0.97	-
	ZERO-DAY		
	☒	AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEV	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:*	-
Apache Tomcat Unauthenticated Remote Code Execution Vulnerability	☒		
	CWE ID	ASSOCIATED TTPs	PATCH LINKS
	CWE-367	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	Apache, Suse, RedHat, Ubuntu, Debian

Vulnerability Details

#1

In January, the Linux ecosystem addressed over 1000 vulnerabilities across various distributions and products, covering critical issues such as information disclosure, privilege escalation, and code execution. Over 650 new vulnerabilities were discovered and patched. HiveForce lab has identified 11 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, Credential Access, Privilege Escalation and Exfiltration. Notably, one of these vulnerabilities are under active exploitation, which require urgent attention and remediation.

#3

Two critical vulnerabilities, CVE-2024-12381 and CVE-2024-12692, in Google Chrome's V8 JavaScript engine underscore the dangers of type confusion. These flaws allow remote attackers to exploit heap corruption and execute arbitrary code via crafted HTML pages. Type confusion, which occurs when resources like pointers or variables are accessed using incompatible types, can lead to logical errors and out-of-bounds memory access. While often associated with C and C++, these issues also affects dynamic languages like PHP or Perl.

#4

Beyond Chrome, CVE-2024-45337 reveals a flaw in the ServerConfig.PublicKeyCallback of certain SSH implementations. This vulnerability enables attackers to bypass public key authentication by manipulating the order of keys sent during authentication. Applications relying on misused third-party libraries or incorrect assumptions in authentication flows are particularly at risk.

#5

Meanwhile, CVE-2024-12084 exposes a critical heap-based buffer overflow in the rsync daemon. This vulnerability arises from improper handling of checksum lengths and can allow attackers to execute arbitrary memory writes. With over 660,000 servers exposed, primarily in China, this flaw poses a significant threat to data integrity and system availability.

#6

Finally, CVE-2024-50379 in Apache Tomcat highlights the risks of inconsistencies between Windows file systems and Tomcat's path validation mechanisms. Attackers can bypass validation, upload malicious JSP files, and execute arbitrary code. This vulnerability relies on non-default configurations, such as enabling write access for the default servlet, and is particularly dangerous in environments with case-insensitive file systems.

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 like V8 engines or 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 like Chrome or GStreamer.

Enforce Dependency Hygiene: Regularly update and patch third-party libraries and frameworks like Apache Tomcat and rsync. Monitor open-source vulnerabilities and restrict the use of outdated dependencies.

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

Apply Emergency Mitigation Measures: In cases where patches are unavailable or immediate deployment is not feasible, implement temporary mitigations such as disabling vulnerable features (e.g., file upload mechanisms or public-key callbacks), applying access restrictions, or using intrusion prevention systems to block exploitation attempts.

Reactive Strategies:

Analyze Endpoint Behavior for Anomalies: Monitor endpoint activities for unusual memory or process behavior. Leveraging advanced EDR solutions can help detect and neutralize risks arising from arbitrary code execution vulnerabilities.

Track Authentication Flow Across Logs: Cross-reference authentication logs from identity providers with application login endpoints. Patterns like repeated login failures followed by successful access to secured resources may indicate authentication bypass attempts.

Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-12381	T1190: Exploit Public-Facing Application T1203: Exploitation for Client Execution T1189: Drive-by Compromise	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software	✓ Suse Debian Fedora
CVE-2024-12692	T1190: Exploit Public-Facing Application T1189: Drive-by Compromise T1203: Exploitation for Client Execution	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software	✓ Freexian Debian Suse Fedora
CVE-2024-45337	T1203: Exploitation for Client Execution T1071: Application Layer Protocol	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1037: Filter Network Traffic	✓ Ubuntu RedHat Suse Fedora
CVE-2024-47540	T1068: Exploitation for Privilege Escalation T1203: Exploitation for Client Execution	DS0009: Process DS0015: Application Log DS0029: Network Traffic	M1051: Update Software M1050: Exploit Protection M1048: Application Isolation and Sandboxing	✓ Ubuntu RedHat Suse Debian Fedora
CVE-2024-50379*	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	DS0015: Application Log DS0029: Network Traffic	M1051: Update Software	✓ Apache Suse RedHat Ubuntu Debian
CVE-2024-12084	T1203: Exploitation for Client Execution	DS0017: Command DS0009: Process	M1051: Update Software	✓ Ubuntu Suse Fedora Debian
CVE-2024-45387	T1190: Exploit Public-Facing Application T1078: Valid Accounts	DS0015: Application Log	M1051: Update Software	✓ Apache Suse

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-56337	T1190: Exploit Public-Facing Application	DS0015: Application Log	M1051: Update Software	✓ Apache Suse Debian RedHat
CVE-2025-0247	T1203: Exploitation for Client Execution	DS0009: Process	M1051: Update Software	✓ Suse RedHat Debian Fedora Ubuntu
CVE-2025-21613	T1203: Exploitation for Client Execution T1059: Command and Scripting Interpreter	DS0015: Application Log DS0029: Network Traffic DS0017: Command DS0009: Process	M1050: Exploit Protection M1038: Execution Prevention	✓ RedHat Suse Debian Oracle Linux
CVE-2024-54534	T1203: Exploitation for Client Exécution T1189: Drive-by Compromise	DS0015: Application Log DS0029: Network Traffic	M1050: Exploit Protection	✓ Ubuntu Debian Suse RedHat

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/

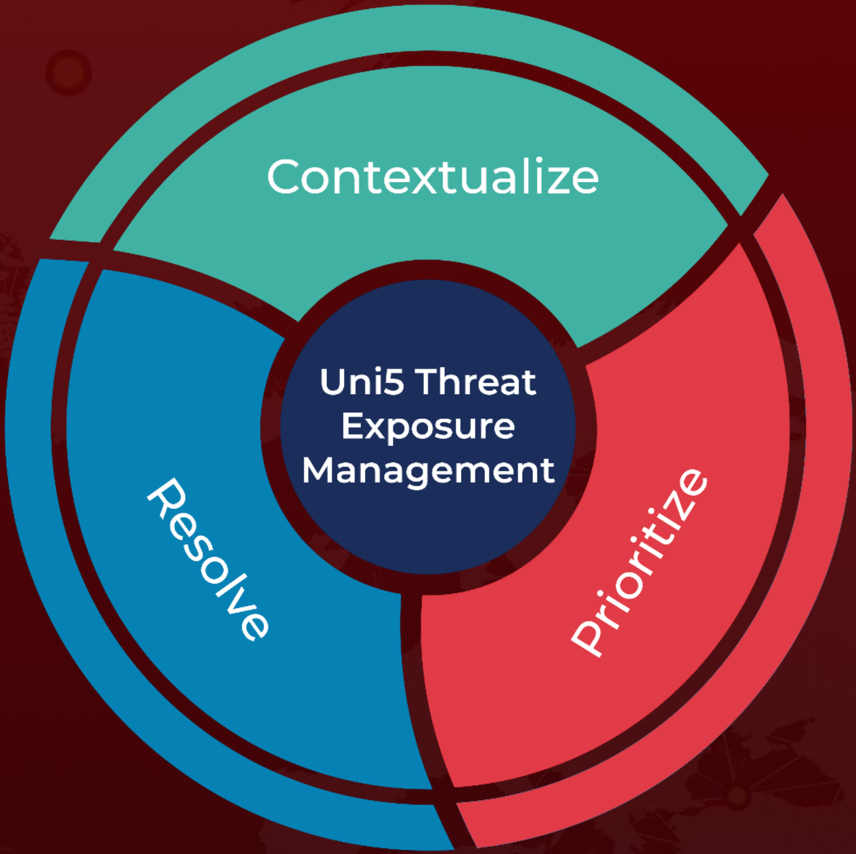
https://access.redhat.com/security/security-updates/

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

January 28, 2025 • 04:30 AM

More at www.hivepro.com