

HiveForce Labs

THREAT ADVISORY



VULNERABILITY REPORT

December 2024 Linux Patch Roundup

Date of Publication

December 19, 2024

Admiralty Code

A1

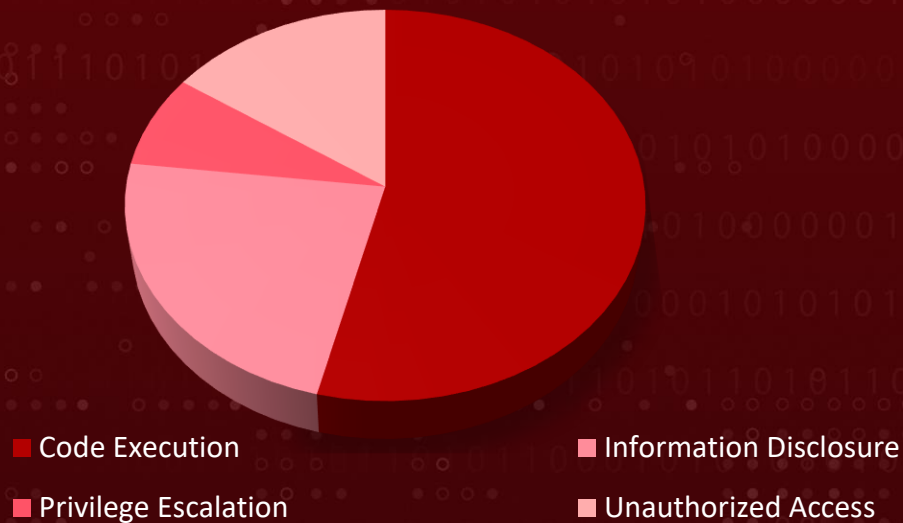
TA Number

TA2024466

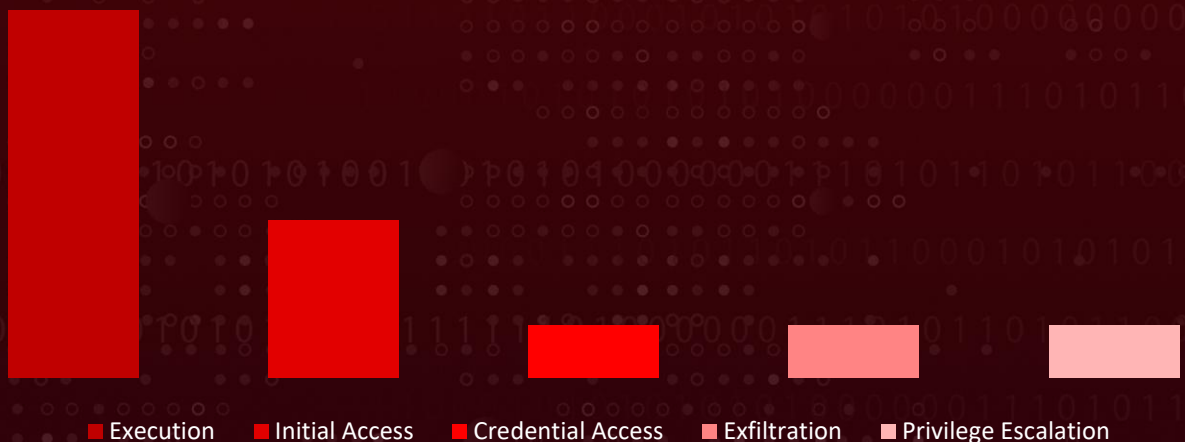
Summary

In November and December, more than 300 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 1,000 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-2024-44308*	WebKitGTK and WPE Webkit Code Execution Vulnerability	WebKitGTK, WPE WebKit, RHEL7, SUSE, Debian, Fedora, macOS	Code Execution	Phishing
CVE-2024-44309*	WebKitGTK and WPE Webkit Cross-Site Scripting (XSS) Vulnerability	WebKitGTK, WPE WebKit, RHEL, SUSE, Debian, Fedora, macOS	Information Disclosure	Phishing
CVE-2024-30896	InfluxDB Operator Token Privilege Escalation Vulnerability	InfluxDB OSS 2.x, RH ACM-Kubernetes, OpenShift Service Mesh	Privilege Escalation	Network
CVE-2024-47533	Cobbler XML-RPC Improper Authentication Vulnerability	Cobbler, SUSE Manager Server, OpenSUSE	Unauthorized Access	Network Unauthenticated
CVE-2024-49369	Icinga Improper TLS Certificate Validation Vulnerability	Icinga 2	Code Execution	Network
CVE-2024-52316	Apache Tomcat Authentication Bypass Vulnerability	Apache Tomcat, SUSE Linux Ent Server, OpenSUSE, SolarWinds Web Help Desk	Unauthorized Access	Remote Unauthenticated
CVE-2024-52317	Apache Tomcat HTTP/2 Data Leakage Vulnerability	Apache Tomcat	Information Disclosure	Remote




* 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-2024-52318	Apache Tomcat Generated JSP XSS Vulnerability	Apache Tomcat	Sensitive Information Disclosure	Remote
CVE-2024-10224	ScanDeps pesky pipe code execution Vulnerability	libmodule-scandeps-perl, Ubuntu, Fedora, Debian, Azure Linux	Code Execution	Local
CVE-2024-11003	needrestart scandeps arbitrary code execution	needrestart, Ubuntu, Fedora	Code Execution	Local
CVE-2024-48990	needrestart PYTHONPATH Arbitrary Code Execution Flaw	needrestart	Code Execution	Local
CVE-2024-48991	needrestart TOCTOU Code Execution Vulnerability	needrestart	Code Execution	Local
CVE-2024-48992	needrestart RUBYLIB Arbitrary Code Execution Flaw	needrestart	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-2024-44308		WebKitGTK, WPE WebKit before 2.46.4, RHEL7, SUSE, Debian, Fedora, macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:suse:*:*:*:*:*:*:*:* *	
WebKitGTK and WPE Webkit Code Execution Vulnerability		cpe:2.3:o:opensuse:leap:*:*:*:*:*:* *:*:*:**	
		cpe:2.3:o:fedoraproject:fedora:*:*:*:*:*:* *:*:*:*:*:*	
	cpe:2.3:o:debian:debian_linux:*:*:*:*:*:* *:*:*:*:*:*		
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-20	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	Debian , Fedora , RedHat , Ubuntu , macOS

CVE ID	CELEBRITY VULNERABILITY	AFFECTED PRODUCTS	ASSOCIATED ACTOR
<u>CVE-2024-44309</u>		WebKitGTK, WPE WebKit before 2.46.4, RHEL, SUSE, Debian, Fedora, macOS	-
	ZERO-DAY		
		AFFECTED CPE	ASSOCIATED ATTACKS/RANSOMWARE
NAME	CISA KEY	cpe:2.3:o:suse:*:*:*:*:*:*:* cpe:2.3:o:opensuse:leap:*:*:*:*:* cpe:2.3:o:fedoraproject:fedora:*:*:*:*:* cpe:2.3:o:debian:debian_linux:*:*:*:*:* cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:* cpe:2.3:o:apple:macos:*:*:*:*	-
WebKitGTK and WPE Webkit Cross-Site Scripting (XSS) Vulnerability			
	CWE ID	ASSOCIATED TTPs	PATCH LINK
	CWE-79	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	<u>Debian</u> , <u>Fedora</u> , <u>RedHat</u> , <u>Ubuntu</u> , <u>macOS</u>

Vulnerability Details

#1

In November and December, 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 300 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, Credential Access, Privilege Escalation and Exfiltration. Notably, two of these vulnerabilities are under active exploitation, which require urgent attention and remediation.

#3

CVE-2024-44308 and CVE-2024-44309 are critical vulnerabilities affecting WebKitGTK and WPE WebKit, which are ports of the WebKit rendering engine used in various Linux distributions and macOS. WebKitGTK is primarily used in desktop environments, while WPE WebKit is optimized for embedded systems. These vulnerabilities, first flagged by Apple as being exploited in the wild as zero-day attacks, pose significant security risks to systems using these WebKit ports for web content rendering.

#4

Apache has released a patch addressing a critical authentication bypass vulnerability in Tomcat. The flaw occurs when Tomcat is configured with a custom Jakarta Authentication (formerly JASPIC) ServerAuthContext component. Improper handling of an authentication exception in this configuration could cause the authentication process to erroneously succeed.

#5

Additionally, Cobbler, a Linux installation server, was found to have an improper authentication flaw. This vulnerability allowed anyone with network access to log in using a default password, potentially enabling them to tamper with installation images and create a supply chain attack scenario.

#6

Finally, Multiple critical vulnerabilities were identified in the needrestart package, a utility widely used in Linux systems. The package was found to be susceptible to the "pesky pipe" technique in Perl, where improper handling of pipes in file operations could lead to arbitrary code execution. Additionally, several other flaws were discovered that could result in code execution with elevated privileges. Alarming, these vulnerabilities are trivial to exploit and have existed for over a decade.

Recommendations

Proactive Strategies:



Exposure Assessment: Conduct an extensive service exposure evaluation with context of active threats to identify any publicly accessible services that may be vulnerable to exploitation. Following this assessment, it is essential to take immediate and decisive action to remediate any identified vulnerabilities by either installing necessary patches or implementing appropriate security measures. This proactive approach will help mitigate potential risks and enhance overall security posture.



User awareness is essential in defending against initial access threats, particularly in light of recent webkit vulnerabilities that require user execution for successful exploitation. These vulnerabilities highlight the importance of educating users about phishing and the identification of malicious activities. Organizations can stay one step ahead of cyber threats by fostering a culture of security hygiene.



XSS Protection: To mitigate the risks associated with CVE-2024-52318, ensure that all JSP outputs are explicitly validated and escaped to prevent XSS vulnerabilities. Implement a comprehensive Content Security Policy (CSP) to block the execution of malicious scripts. Regularly audit and update your codebase to identify and address potential security gaps.



Limit Exposure: Minimizing service exposure is an effective strategy to reduce the risks associated with CVE-2024-30896, CVE-2024-47533, and CVE-2024-49369. By limiting access to only what is necessary, organizations can reduce the attack surface and enhance the overall security. However, CVE-2024-47533 poses a substantial risk due to its nature as an unauthenticated exploit.

Reactive Strategies:




Monitor endpoints for unusual library loads, as this can indicate potential threats. Utilizing EDR solutions can aid in detecting and mitigating code execution risks linked to needrestart packages.









Correlate identity provider authentication logs with Tomcat login endpoint activity. Failed authentication attempts in the auth database, followed by the same session accessing post-login pages, strongly indicate a successful bypass of the application authentication process.



Detect, Mitigate & Patch

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-44308	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	DS0015: Application Log Content DS0009: Process Creation	M1048: Application Isolation and Sandboxing M1017: User Training	 Debian, Fedora, RedHat, Ubuntu, macOS
CVE-2024-44309	T1189: Drive-by compromise T1204.001: User Execution: Malicious Link	DS0015: Application Log Content DS0029: Network Connection Creation	M1048: Application Isolation and Sandboxing M1017: User Training	 Debian, Fedora, RedHat, Ubuntu, macOS
CVE-2024-30896	T1528: Steal Application Access Token T1565 : Data Manipulation	DS0028: Logon Session Metadata	M1018: User Account Management	
CVE-2024-47533	T1078: Valid Accounts	DS0028: Logon Session Creation	M1051: Update Software	 Cobbler, SUSE
CVE-2024-49369	T1190: Exploit Public-Facing Application T1203: Exploitation for Client Execution	DS0015: Application Log Content	M1051: Update Software	 Link
CVE-2024-52316	T1190: Exploit Public-Facing Application	DS0015: Application Log Content	M1050: Exploit Protection	 Apache, SUSE, SolarWinds
CVE-2024-52317	T1190: Exploit Public-Facing Application	DS0015: Application Log Content	M1050: Exploit Protection	 Link

CVE ID	TTPs	Detection	Mitigation	Patch
CVE-2024-52318	T1539: Steal Web Session Cookie T1189: Drive-by Compromise T1566: Phishing	<u>DS0015: Application Log Content</u>	<u>M1050: Exploit Protection</u>	 Link
CVE-2024-10224	T1068: Exploitation for Privilege Escalation	<u>DS0017: Command Execution</u> <u>DS0009: Process Creation</u>	<u>M1038: Execution Prevention</u> <u>M1051: Update Software</u>	 Ubuntu, Fedora, Debian, Azure Linux
CVE-2024-11003	T1068: Exploitation for Privilege Escalation T1203: Exploitation for Client Execution	<u>DS0017: Command Execution</u> <u>DS0009: Process Creation</u>	<u>M1038: Execution Prevention</u> <u>M1051: Update Software</u>	 Ubuntu, Fedora
CVE-2024-48990				 Ubuntu, Fedora
CVE-2024-48991	T1059: Command and Scripting Interpreter T1574: Hijack Execution Flow	<u>DS0017: Command Execution</u> <u>DS0009: Process Creation</u>	<u>M1038: Execution Prevention</u> <u>M1040: Behavior Prevention on Endpoint</u>	 Ubuntu, Fedora
CVE-2024-48992				 Ubuntu, Fedora

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/>

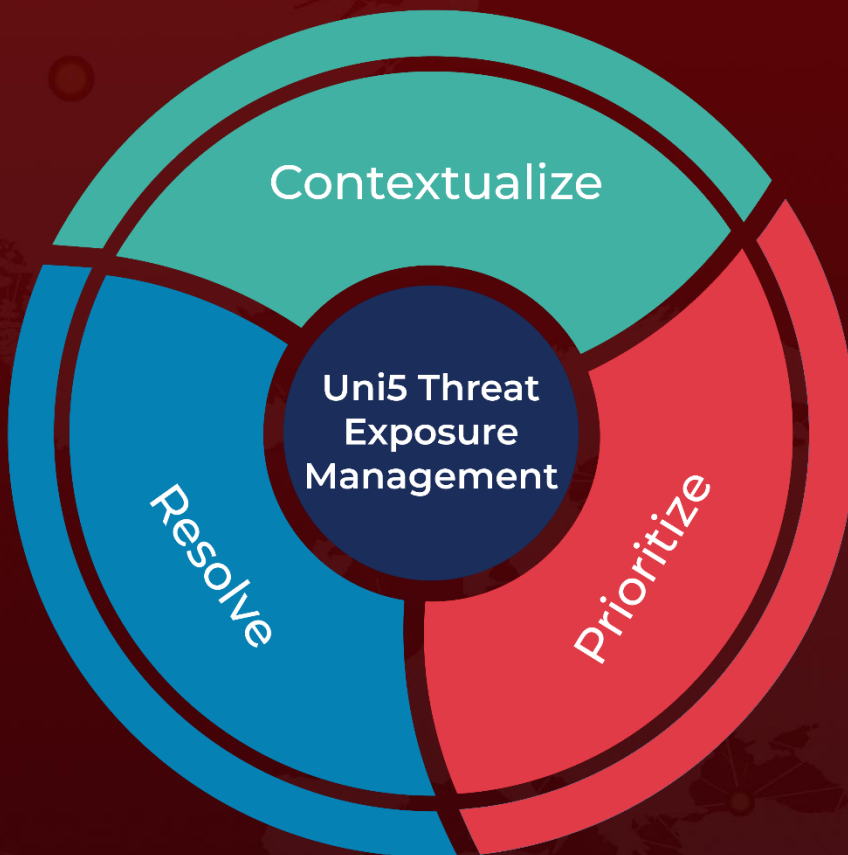
<https://access.redhat.com/security/security-updates/>

<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

December 19, 2024 • 02:00 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com