Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

New Apache Vulnerabilities Could Be a Hacker's Playground

Date of Publication	Admiralty Code	TA Number
December 26, 2024	A1	TA2024472

Summary

Discovered On: December 2024
Affected Products: Tomcat, Traffic Control
Impact: The Apache Software Foundation (ASF) has uncovered critical vulnerabilities in Apache Tomcat and Traffic Control, putting systems at risk of remote code execution and database compromise. These flaws exploit timing gaps and SQL injection techniques, potentially disrupting key operations and exposing sensitive data. Organizations are urged to act swiftly, apply updates, and fortify their defenses to prevent catastrophic impacts on their infrastructure.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2024-56337	Apache Tomcat Remote Code Execution Vulnerability	Apache Tomcat	✗	✗	✓
CVE-2024-45387	Apache SQL Injection Vulnerability	Apache Traffic Control	✗	✗	✓

Vulnerability Details

#1 The Apache Software Foundation (ASF) has issued a security update to address a significant vulnerability in its Tomcat server software. Tracked as CVE-2024-56337, this flaw is an incomplete mitigation of a previously resolved vulnerability, CVE-2024-50379, which was addressed on December 17, 2024. The vulnerability could lead to remote code execution (RCE) under specific conditions, posing a critical risk to systems.

#2 Apache Tomcat, an open-source web server and servlet container, is extensively used to deploy Java-based web applications. It provides a runtime environment for Java Servlets, JavaServer Pages (JSP), and Java WebSocket technologies, making it a cornerstone of many enterprises.

#3 The issue arises from a Time-of-Check to Time-of-Use (TOCTOU) race condition within Tomcat's default servlet. On case-insensitive file systems with write permissions enabled, Tomcat performs a safety check on files. However, an attacker can exploit the time gap between the check and use by renaming or altering files, enabling malicious JSP files to bypass these checks under high concurrency. This bypass could result in executing malicious code, particularly in environments experiencing concurrent file uploads and reads.

#4 ASF has also addressed a critical SQL injection vulnerability in its Traffic Control platform, tracked as CVE-2024-45387. Apache Traffic Control is a popular open-source solution for managing large-scale content delivery networks (CDNs). This vulnerability enables a privileged user with roles such as "admin," "federation," "operations," "portal," or "steering" to execute arbitrary SQL commands on the database through a specially crafted PUT request.

#5 Exploiting this flaw could have severe repercussions, including unauthorized access to sensitive data, manipulation or deletion of database records, privilege escalation, and even full compromise of the affected infrastructure. Such an attack could significantly disrupt CDN operations and compromise the integrity of managed networks.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-56337	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	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*:*	CWE-367
CVE-2024-45387	Apache Traffic Control 8.0.0 through 8.0.1	cpe:2.3:a:apache:traffic_control:*:*:*:*:*:*:*:*	CWE-285 CWE-89

Recommendations

Upgrade Apache Tomcat: While upgrading to the latest Apache Tomcat versions (11.0.2, 10.1.34, and 9.0.98) is critical, additional configuration steps are necessary to fully mitigate the risk.

Java Configuration Adjustments:

- For Java 8 or 11, set the system property sun.io.useCanonCaches to false (default is true).
- For Java 17, confirm that sun.io.useCanonCaches is set to false (default is already false).
- For Java 21 and later, no action is required as the problematic cache has been removed.

Disable Default Servlet Write Access: By default, Tomcat's default servlet is set to read-only. If your environment does not require runtime file uploads, ensure that this parameter remains disabled to prevent unauthorized file modifications.

Mitigation Measures for CVE-2024-45387: If an immediate update to address CVE-2024-45387 is not possible, several interim measures can help mitigate the risk. First, restrict access to Traffic Ops for users with affected roles, including "admin," "federation," "operations," "portal," or "steering."

Additionally, actively **monitor logs** for any suspicious database queries or unusual activities that may suggest exploitation attempts. It is also crucial to enhance the security of custom scripts by implementing input validation and utilizing parameterized queries to prevent SQL injection. Lastly, enforce the principle of least privilege by limiting user roles and permissions to reduce the attack surface until a full patch is applied.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0040 Impact	**T1059** Command and Scripting Interpreter	**T1203** Exploitation for Client Execution	**T1505** Server Software Component
T1027 Obfuscated Files or Information	**T1190** Exploit Public-Facing Application	**T1565** Data Manipulation	

Patch Details

The CVE-2024-56337 vulnerability has been addressed in Apache Tomcat versions 11.0.2, 10.1.34, and 9.0.98. However, users should refer to the additional recommendations, as certain Java configurations may still require manual adjustments.

For the CVE-2024-45387 vulnerability, users are advised to upgrade to Apache Traffic Control version 8.0.2 if running an affected version of Traffic Ops.

Links:
https://tomcat.apache.org/security-11.html
https://tomcat.apache.org/security-10.html
https://tomcat.apache.org/security-9.html
https://trafficcontrol.apache.org/releases/

References

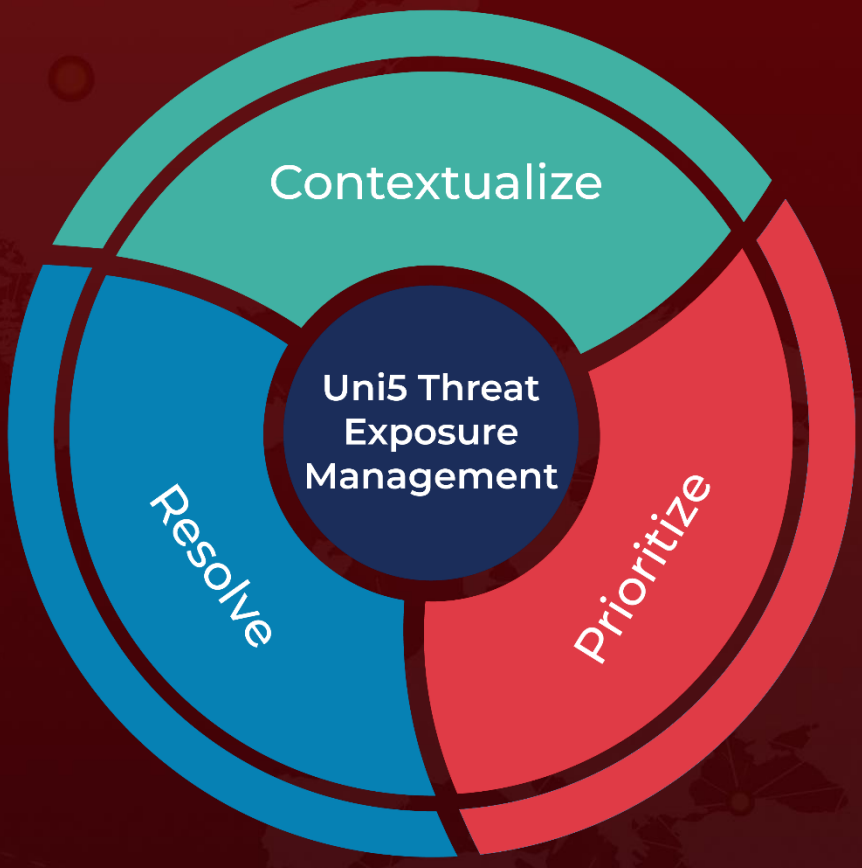
https://lists.apache.org/thread/2bjnh3p78b89n5hw539hh31sr7tt7m22

https://lists.apache.org/thread/t38nk5n7t8w3pb66z7z4pqfzt4443trr

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 26, 2024 • 5:00 AM

More at www.hivepro.com