Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Flaw in Apache Tomcat Poses DoS Risk, Threatening Service Availability

Date of Publication	Admiralty Code	TA Number
September 25, 2024	A1	TA2024371

Summary

First Seen: June 2024
Affected Products: Apache Tomcat
Impact: Apache Tomcat has been found to contain a newly discovered vulnerability, CVE-2024-38286, which could allow attackers to exploit the TLS handshake process to launch Denial of Service (DoS) attacks. By targeting this critical mechanism, attackers can overwhelm system resources, potentially leading to service disruptions. To mitigate the risk, users are urged to update their Apache Tomcat instances to the latest versions.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2024-38286	Apache Tomcat Denial of Service Vulnerability	Apache Tomcat	✗	✗	✓

Vulnerability Details

#1

The Apache Software Foundation has released a security advisory regarding a newly identified vulnerability in Apache Tomcat, CVE-2024-38286, which could enable attackers to carry out Denial-of-Service (DoS) attacks. This vulnerability, rated as Important, impacts multiple versions of Apache Tomcat across all platforms. Attackers can exploit this flaw by manipulating the TLS handshake process, potentially overwhelming system resources and disrupting services.

#2 The CVE-2024-38286 vulnerability arises from improper control over internal resource consumption during the TLS handshake process in Apache Tomcat. A remote attacker can exploit this flaw by initiating multiple TLS connections, leading to memory exhaustion and triggering a Denial-of-Service (DoS) attack. Under certain configurations, this vulnerability can cause an OutOfMemoryError, severely impacting the availability of affected systems. Attackers exploiting this flaw can degrade or completely disrupt services, posing a significant risk to system availability.

#3 To mitigate the risks posed by CVE-2024-38286, organizations using Apache Tomcat must promptly apply the recommended patches. Ensuring systems are updated will prevent attackers from exploiting this vulnerability to disrupt service availability.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-38286	Apache Tomcat 11.0.0-M1 to 11.0.0-M20 Apache Tomcat 10.1.0-M1 to 10.1.24 Apache Tomcat 9.0.13 to 9.0.89	cpe:2.3:a:apache:tomcat:*:*:*:*:*:*:*	CWE-400

Recommendations

Update: Users of the affected versions of Apache Tomcat servers should immediately update to the fixed releases. Applying these updates is crucial to safeguard against vulnerabilities and maintain the security of your Tomcat servers.

Implement Web Application Firewall (WAF): Deploy a WAF to monitor and filter incoming web traffic. A properly configured WAF can detect and block attempts to exploit the vulnerabilities, providing an additional layer of protection.

Review Configuration Settings: Review your TLS settings and ensure they are configured securely. Disable any unnecessary protocols or ciphers that may expose your server to risks. Implement resource limits for connections and threads in your server configuration to help mitigate the impact of potential DoS attacks.

Implement Monitoring and Logging: Ensure that logging is enabled for your Tomcat server to capture detailed information about incoming requests and any errors that occur. Regularly monitor CPU and memory usage on your server to detect unusual patterns that may indicate an ongoing attack.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0040 Impact	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1498 Network Denial of Service			

Patch Details

Users of the affected Apache Tomcat versions are strongly urged to apply one of the following patches to mitigate the vulnerability.

For Apache Tomcat 11: Upgrade to 11.0.0-M21 or later.
For Apache Tomcat 10.1: Upgrade to 10.1.25 or later.
For Apache Tomcat 9.0: Upgrade to 9.0.90 or later.

Patch Links:
https://tomcat.apache.org/download-11.cgi
https://tomcat.apache.org/download-10.cgi
https://tomcat.apache.org/download-90.cgi

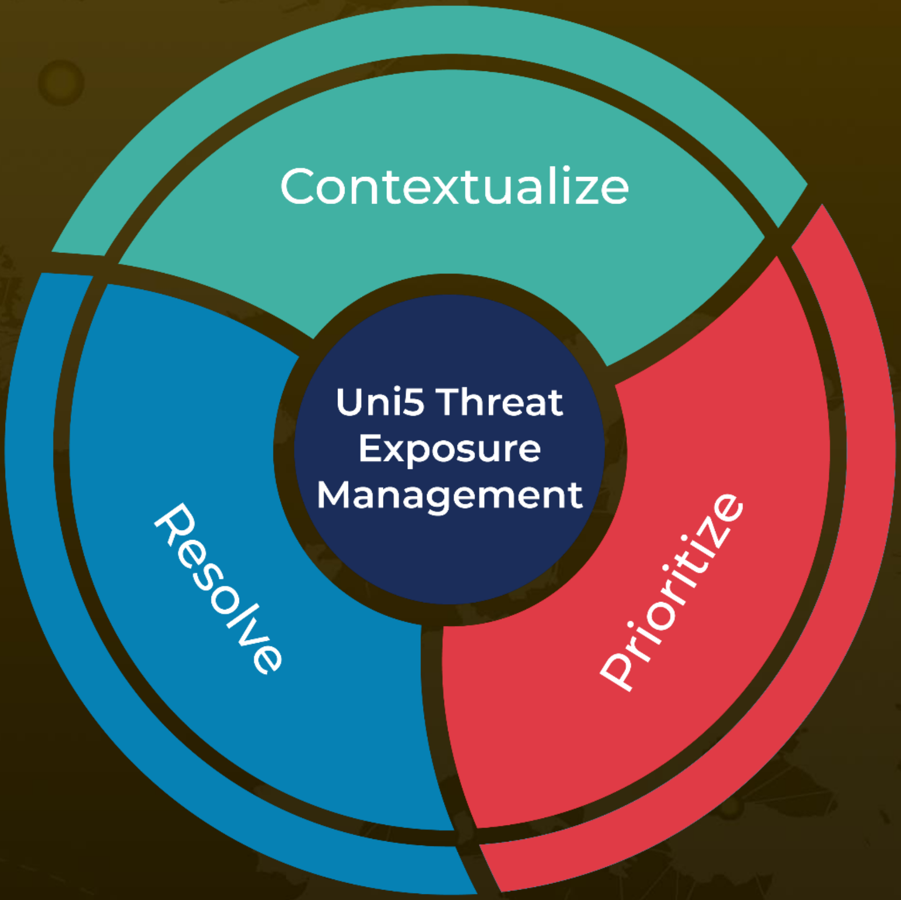
References

https://lists.apache.org/thread/8xm50bvr6rhbjkdtbxl5x4d20dpfy83p

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

September 25, 2024 • 6:00 AM

More at www.hivepro.com