TLP: WHITE

Advisory Alert

Alert Number: AAA20241223 **Date:** December 23, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Apache Tomcat	**High**	Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-49995, CVE-2024-50290, CVE-2024-53063)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to string buffer overrun, overflows on SNR calculus, out of memory access. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SUSE Linux Enterprise Server 11 SP4 SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20244397-1/

Affected Product	**Apache Tomcat**
Severity	**High**
Affected Vulnerability	Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability (CVE-2024-56337)
Description	Apache has released security updates addressing a Time-of-check Time-of-use (TOCTOU) Race Condition Vulnerability that exists in Apache Tomcat. **CVE-2024-56337 -** A Time-of-Check Time-of-Use (TOCTOU) Race Condition vulnerability exists in Apache Tomcat when running on case-insensitive file systems with the write-enabled Default Servlet. If exploited, a malicious user could execute remote code. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat 11 versions 11.0.0-M1 to 11.0.1 Apache Tomcat 10 versions 10.1.0-M1 to 10.1.33 Apache Tomcat 9 versions 9.0.0.M1 to 9.0.97
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.2 • https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.34 • https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.98

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-24490,CVE-2024-40910,CVE-2024-35965,CVE-2024-26822,CVE-2024-40973,CVE-2020-12352,CVE-2024-35967,CVE-2024-38553,CVE-2024-35963,CVE-2020-12351,CVE-2024-35966,CVE-2024-50264,CVE-2024-53057,CVE-2024-43904)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7179-1

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.