# Advisory Alert

**Alert Number:** AAA20250915 **Date:** September 15, 2025

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Apache Tomcat** | **High** | Improper Resource Shutdown or Release Vulnerability |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **IBM** | **High**, Medium, Low | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Apache Tomcat** |
| Severity | **High** |
| Affected Vulnerability | Improper Resource Shutdown or Release vulnerability (CVE-2025-48989) |
| Description | Apache has released security updates addressing an Improper Resource Shutdown or Release Vulnerability that exists in Apache Tomcat.<br>**CVE-2025-48989** - Improper Resource Shutdown or Release vulnerability in Apache Tomcat HTTP/2 implementation made Tomcat vulnerable to the made you reset attack. The denial of service typically manifested as an OutOfMemoryError.<br>Apache advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Apache Tomcat 11.x versions 11.0.0-M1 to 11.0.9<br>Apache Tomcat 10.x versions 10.1.0-M1 to 10.1.43<br>Apache Tomcat 9.x versions 9.0.0.M1 to 9.0.107 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://tomcat.apache.org/security-11.html<br>• https://tomcat.apache.org/security-10.html<br>• https://tomcat.apache.org/security-9.html |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | SUSE 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.<br>SUSE advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | openSUSE Leap 15.5<br>SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5<br>SUSE Linux Enterprise Live Patching 12-SP5, 15-SP5<br>SUSE Linux Enterprise Micro 5.5<br>SUSE Linux Enterprise Real Time 15 SP5<br>SUSE Linux Enterprise Server 12 SP5, 15 SP5<br>SUSE Linux Enterprise Server 12 SP5 LTSS<br>SUSE Linux Enterprise Server 12 SP5 LTSS Extended Security<br>SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2025/suse-su-202503204-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503195-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503194-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503191-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503190-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503188-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503185-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-202503186-1/ |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **High**, Medium, Low |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-22097, CVE-2025-37914, CVE-2025-38250, CVE-2025-38380, CVE-2023-49083, CVE-2025-8194, CVE-2025-6032, CVE-2025-5994, CVE-2021-47670, CVE-2024-56644, CVE-2025-21727, CVE-2025-21759, CVE-2025-38085, CVE-2025-38159, CVE-2025-22058, CVE-2025-38200, CVE-2025-5914, CVE-2025-6020, CVE-2025-0164) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. These vulnerabilities could be exploited by malicious users cause Denial of Service, Privilege Escalation, Arbitrary Code Execute, memory corruption.<br>IBM advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | IBM QRadar SIEM versions 7.5 - 7.5.0 UP13 IF01 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.ibm.com/support/pages/node/7244786<br>• https://www.ibm.com/support/pages/node/7244784 |

### 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.**