# Advisory Alert

**Alert Number:** AAA20250403 **Date:** April 3, 2025

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Red Hat** | **High** | Security Update |
| **SUSE** | **High** | Multiple Vulnerabilities |
| **Ubuntu** | **High** | Multiple Vulnerabilities |
| **Cisco** | **High**, **Medium** | Multiple Vulnerabilities |
| **Drupal** | **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Red Hat** |
| Severity | **High** |
| Affected Vulnerability | Security Update (CVE-2025-24813) |
| Description | Red Hat has released security updates addressing a vulnerability that exists in Apache Tomcat which affects JBoss Enterprise Web Server.<br>**CVE-2025-24813** - A flaw was found in Apache Tomcat. In certain conditions and configurations, this vulnerability allows a remote attacker to exploit a path equivalence flaw to view file system contents and add malicious content via a write-enabled Default Servlet in Apache Tomcat.<br>Red Hat advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | JBoss Enterprise Web Server Text-Only Advisories x86_64<br>JBoss Enterprise Web Server 5 for RHEL 9 x86_64<br>JBoss Enterprise Web Server 5 for RHEL 8 x86_64<br>JBoss Enterprise Web Server 5 for RHEL 7 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://access.redhat.com/errata/RHSA-2025:3455<br>• https://access.redhat.com/errata/RHSA-2025:3454 |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-41062, CVE-2022-49025, CVE-2022-48791) |
| 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 15.3, 15.4, 15.5<br>SUSE Linux Enterprise High Performance Computing 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Live Patching 15-SP3, 15-SP4, 15-SP5<br>SUSE Linux Enterprise Micro 5.1, 5.2, 5.3, 5.4, 5.5<br>SUSE Linux Enterprise Real Time 15 SP4, 15 SP5<br>SUSE Linux Enterprise Server 15 SP3, 15 SP4, 15 SP5<br>SUSE Linux Enterprise Server for SAP Applications 15 SP3, 15 SP4, 15 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2025/suse-su-20251104-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-20251114-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-20251119-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-20251120-1/<br>• https://www.suse.com/support/update/announcement/2025/suse-su-20251121-1/ |

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-56658, CVE-2024-35864, CVE-2024-26928, CVE-2024-57798) |
| Description | Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to cause privilege escalation, system crash and use-after-free conditions.<br>Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Ubuntu 22.04<br>Ubuntu 20.04<br>Ubuntu 18.04 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://ubuntu.com/security/notices/USN-7408-1<br>• https://ubuntu.com/security/notices/USN-7406-1 |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-20139, CVE-2025-20212, CVE-2025-20120, CVE-2025-20203) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service and Cross-Site Scripting.<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Cisco Enterprise Chat and Email Releases 12.6, 12.5 and prior<br>Cisco Meraki MX Firmware Releases 19.1, 18.2, 18.1, 17 and 16.2<br>Cisco EPNM Releases 8.0, 7.1, 6.1 and prior<br>Cisco Prime Infrastructure Releases 3.10, 3.9 and prior |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-dos-tC6m9GZ8<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-vNRpDvfb<br>• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnmpi-sxss-GSScPGY4 |

| | |
|---|---|
| Affected Product | **Drupal** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2025-3129, CVE-2025-3130) |
| Description | Drupal has released security updates addressing multiple vulnerabilities that exist in their products.<br>**CVE-2025-3129** - The module doesn't sufficiently protect against brute force attacks to guess a user's access code.<br>**CVE-2025-3130** - The module doesn't sufficiently sanitize input when ROT13 encoding is used. This vulnerability is mitigated by the fact that an attacker must have a role with the ability to enter specific HTML tag attributes. In a default Drupal installation this would require the administrator role and use of the Full HTML text format. It also requires that the ROT13 encoding be enabled in Obfuscate settings.<br>Drupal advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | access_code versions prior to 2.0.4 for Drupal 8.x or later<br>Obfuscate versions prior to 2.0.1 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.drupal.org/sa-contrib-2025-028<br>• https://www.drupal.org/sa-contrib-2025-029 |

**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.**