# Advisory Alert

**Alert Number:** **AAA20230518** **Date:** **May 18, 2023**

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

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **Critical** | Multiple Vulnerabilities |
| **Redhat** | **High** | Multiple Vulnerabilities |
| **Suse** | **High** | Multiple Vulnerabilities |
| **IBM** | **Medium**, **Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-20024, CVE-2023-20156, CVE-2023-20157, CVE-2023-20158, CVE-2023-20159, CVE-2023-20160, CVE-2023-20161, CVE-2023-20162, CVE-2023-20189) |
| Description | Cisco has released a security update addressing multiple vulnerabilities that exist in Cisco switches. Successful exploitation of these vulnerabilities could cause Heap Buffer Overflow, Stack Buffer Overflow, BSS Buffer Overflow, Denial-of-Service and Unauthenticated Configuration Reading<br>Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | 250 Series Smart Switches<br>350 Series Managed Switches<br>350X Series Stackable Managed Switches<br>550X Series Stackable Managed Switches<br>Business 250 Series Smart Switches<br>Business 350 Series Managed Switches<br>Small Business 200 Series Smart Switches<br>Small Business 300 Series Managed Switches<br>Small Business 500 Series Stackable Managed Switches |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sg-web-multi-S9g4Nkgv |

| | |
|---|---|
| Affected Product | **Redhat** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-22970, CVE-2022-22971, CVE-2022-3782, CVE-2023-0461, CVE-2023-0482, CVE-2023-1390, CVE-2023-20860, CVE-2023-20861) |
| Description | Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Bypass access validation, Privilege escalation, Denial of service and Unauthenticated reads by a local user.<br>Redhat recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64<br>Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le<br>Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://access.redhat.com/errata/RHSA-2023:3185<br>https://access.redhat.com/errata/RHSA-2023:3190 |

| | |
|---|---|
| Affected Product | **Suse** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2017-5753, CVE-2020-36691, CVE-2021-3923, CVE-2021-4203, CVE-2022-20567, CVE-2022-2196, CVE-2022-43945, CVE-2023-0386, CVE-2023-0590, CVE-2023-0597, CVE-2023-1076, CVE-2023-1095, CVE-2023-1118, CVE-2023-1390, CVE-2023-1513, CVE-2023-1611, CVE-2023-1670, CVE-2023-1855, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2008, CVE-2023-2019, CVE-2023-2124, CVE-2023-2162, CVE-2023-2176, CVE-2023-2235, CVE-2023-23006, CVE-2023-23454, CVE-2023-23455, CVE-2023-2483, CVE-2023-28328, CVE-2023-28464, CVE-2023-28772, CVE-2023-30772) |
| Description | Suse has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Local privilege escalation, Buffer overflow, Denial of service, remote DoS<br>Suse recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | openSUSE Leap 15.4<br>openSUSE Leap Micro 5.3<br>SUSE Linux Enterprise High Availability Extension 12 SP4<br>SUSE Linux Enterprise High Performance Computing 12 SP4, 15 SP4<br>SUSE Linux Enterprise Live Patching 12-SP4, 15-SP4<br>SUSE Linux Enterprise Micro 5.3, 5.4<br>SUSE Linux Enterprise Micro for Rancher 5.3, 5.4<br>SUSE Linux Enterprise Real Time 15 SP4<br>SUSE Linux Enterprise Server 12 SP4, 15 SP4<br>SUSE Linux Enterprise Server 12 SP4 ESPOS 12-SP4<br>SUSE Linux Enterprise Server 12 SP4 LTSS 12-SP4<br>SUSE Linux Enterprise Server for SAP Applications 12 SP4, 15 SP4<br>SUSE OpenStack Cloud 9<br>SUSE OpenStack Cloud Crowbar 9<br>SUSE Real Time Module 15-SP4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2023/suse-su-20232231-1/<br>https://www.suse.com/support/update/announcement/2023/suse-su-20232232-1/ |

| | |
|---|---|
| Affected Product | **IBM** |
| Severity | **Medium, Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-21426, CVE-2022-21624, CVE-2022-21626, CVE-2022-3676, CVE-2023-21830, CVE-2023-27554) |
| Description | IBM has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Denial of service, Security restriction bypass, Sensitive information disclosure.<br>IBM recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | WebSphere Service Registry and Repository 8.5.x<br>WebSphere Service Registry and Repository Studio 8.5.x<br>WebSphere Application Server v9.0.0.5 shipped with IBM Security Key Lifecycle Manager (SKLM) v3.0, (SKLM) v3.0.1<br>WebSphere Application Server v9.0.5.0 shipped with IBM Security Key Lifecycle Manager (SKLM) v4.0<br>WebSphere Application Server v9.0.5.5 shipped with IBM Security Guardium Key Lifecycle Manager (GKLM) v4.1<br>Websphere Application Server V8.5 and V9 shipped with WebGUI 8.1.0 GA and FP |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.ibm.com/support/pages/node/6995185<br>https://www.ibm.com/support/pages/node/6994249<br>https://www.ibm.com/support/pages/node/6994793 |

**Disclaimer**

**The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.**