# Advisory Alert

**Alert Number:** AAA20230817 **Date:** August 17, 2023

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Suse** | **High** | Multiple Vulnerabilities |
| **Cisco** | **High**, **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Suse** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-40982, CVE-2023-0459, CVE-2023-20569, CVE-2023-20593, CVE-2023-21400, CVE-2023-2156, CVE-2023-2166, CVE-2023-2985, CVE-2023-31083, CVE-2023-3117, CVE-2023-31248, CVE-2023-3268, CVE-2023-3390, CVE-2023-35001, CVE-2023-3567, CVE-2023-3609, CVE-2023-3611, CVE-2023-3776, CVE-2023-3812, CVE-2023-4004, CVE-2023-3776, CVE-2018-20784, CVE-2018-3639, CVE-2023-1637, CVE-2023-3106, CVE-2017-18344, CVE-2022-45919, CVE-2023-3141, CVE-2023-3159, CVE-2023-3161, CVE-2023-35824) |
| Description | Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could to information leakage, out-of-bounds memory access, memory corruptions, side channel attack.<br><br>Suse recommends to apply the necessary security fixes at your earliest to avoid issues. |
| Affected Products | openSUSE Leap 15.4<br>openSUSE Leap Micro 5.3, 5.4<br>SUSE Linux Enterprise High Performance Computing 12 SP2, 12 SP5, 15 SP4<br>SUSE Linux Enterprise Live Patching 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 12 SP5, 15 SP4<br>SUSE Linux Enterprise Server 11 SP4<br>SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE 11-SP4<br>SUSE Linux Enterprise Server 12 SP2<br>SUSE Linux Enterprise Server 12 SP2 BCL 12-SP2<br>SUSE Linux Enterprise Server 12 SP5<br>SUSE Linux Enterprise Server 15 SP4<br>SUSE Linux Enterprise Server for SAP Applications 15 SP4<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-20233318-1/<br>https://www.suse.com/support/update/announcement/2023/suse-su-20233329-1/<br>https://www.suse.com/support/update/announcement/2023/suse-su-20233324-1/<br>https://www.suse.com/support/update/announcement/2023/suse-su-20233333-1/ |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-20228, CVE-2023-20242, CVE-2023-20209, CVE-2023-20237, CVE-2023-20221, CVE-2023-20111, CVE-2023-20013, CVE-2023-20017, CVE-2023-20201, CVE-2023-20203, CVE-2023-20205, CVE-2023-20222, CVE-2023-20217, CVE-2023-20232, CVE-2017-6679, CVE-2023-20212, CVE-2023-20197, CVE-2023-20211, CVE-2023-20229, CVE-2023-20224) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Privilege escalation, Arbitrary file write, SQL Injection, Denial of Service.<br><br>Cisco recommends to apply the necessary security updates at earliest to avoid issues. |
| Affected Products | Cisco 5000 Series ENCS 2.9 and earlier, 3.1, 3.2<br>Cisco Duo Device Health Application for Windows Release 5.0.0, 5.1.0<br>Cisco EPNM Release Earlier than 7.1<br>Cisco Expressway Series and Cisco TelePresence VCS Release Earlier than 14.0, 14.0<br>Cisco Intersight Private Virtual Appliance Release 1.0.9<br>Cisco Intersight Virtual Appliance Release 1.0.9-503 through 1.0.9-558<br>Cisco ISE Release 2.6 and earlier, 2.7, 3.0, 3.1<br>Cisco Prime Infrastructure Release Earlier than 3.10.4<br>Cisco ThousandEyes Enterprise Agent Release 0.216 and earlier<br>Cisco UCS C-Series M5 Rack Server 4.1 and earlier, 4.2<br>Cisco UCS E-Series M3 Server 3.2 and earlier<br>Cisco Umbrella Virtual Appliance Release 2.0.3 and earlier<br>Cisco Unified CCX Release Earlier than 12.5(1)SU03 ES02<br>Cisco Unified CM, Unified CM SME, and Unified CM IM&P Software Release 11.5(1), 12.5(1), 14<br>IP Phone 6800, 7800, and 8800 Multiplatform Firmware 11.3 and earlier<br>Cisco Secure Endpoint Connector for Linux Prior to version 1.22.0<br>Cisco Secure Endpoint Connector for MacOS Prior to version 1.22.0<br>Cisco Secure Endpoint Connector for Windows Prior to version 8.1.7.21585<br>Cisco Secure Endpoint Private Cloud Prior to version 3.8.0<br>Video Phone 8875 - Cisco PhoneOS Release 1.0 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-UMYtYEtr<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imp-xss-QtT4VdsK<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-injection-X475EbTQ<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-intersight-forward-C45ncgqb<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-csrf-HOCmXW2c<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-credentials-tkTO3h3<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ivpa-cmdinj-C5XRbbOy<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-BFjSRJP5<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-storedxss-tTjO62r<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-va-priv-esc-PUdgrx8E<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-wcp-JJeqDT3S<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-umbrella-tunnel-gJw5thgE<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-FTkhqMWZ<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-rNwNEEee<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-injection-g6MbwH2<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-duo-dha-filewrite-xPMBMZAK<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thoueye-privesc-NVhHGwb3 |

**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.**