# Advisory Alert

**Alert Number:** **AAA20231023** **Date:** **October 23, 2023**

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

**Information Classification Level** : TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **Critical** | Privilege Escalation Vulnerabilities |
| **Suse** | **High** | Multiple Vulnerabilities |
| **Solarwinds** | **High** | Multiple Vulnerabilities |
| **VMware** | **High** | Multiple Vulnerabilities |
| **Qnap** | **High** | OS Command Injection Vulnerability |
| **Ubuntu** | **High, Medium, Low** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Critical** |
| Affected Vulnerability | Privilege Escalation Vulnerabilities (CVE-2023-20198, CVE-2023-20273) |
| Description | Cisco has released a security remediation to address privilege escalation vulnerabilities in Cisco IOS XE Software. These vulnerabilities may initially allow an attacker to create a local user and password combination. After creating the local account the attacker may elevate privilege to root and write the implant to the file system.<br>It is strongly recommends to apply the necessary remediation at your earliest to avoid issues. |
| Affected Products | Cisco IOS XE Software if the web UI feature is enabled<br>• Cisco IOS XE Software Release Train 17.9 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z |

| | |
|---|---|
| Affected Product | **Suse** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2020-36766, CVE-2023-1192, CVE-2023-1206, CVE-2023-1859, CVE-2023-2177, CVE-2023-4004, CVE-2023-40283, CVE-2023-42753, CVE-2023-4389, CVE-2023-4622, CVE-2023-4623, CVE-2023-4881, CVE-2023-4921) |
| Description | Suse has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Information disclosure, Denial of service, System crash, Local privilege escalation.<br>Suse recommends to apply the necessary security fixes at your earliest to avoid issues. |
| Affected Products | SUSE Linux Enterprise Micro 5.1<br>SUSE Linux Enterprise Micro 5.2<br>SUSE Linux Enterprise Micro for Rancher 5.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.suse.com/support/update/announcement/2023/suse-su-20234142-1/ |

| | |
|---|---|
| Affected Product | **Solarwinds** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-35180, CVE-2023-35181, CVE-2023-35182, CVE-2023-35183, CVE-2023-35184, CVE-2023-35185, CVE-2023-35186, CVE-2023-35187) |
| Description | Solarwinds has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Remote Code Execution, Privilege Escalation and Directory Traversal.<br>Solarwinds recommends to apply the necessary security fixes at your earliest to avoid issues. |
| Affected Products | Solarwinds Access Rights Manager 2023.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://documentation.solarwinds.com/en/success_center/arm/content/release_notes/arm_2023-2-1_release_notes.htm |

| | |
|---|---|
| Affected Product | **VMware** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-34044, CVE-2023-34045, CVE-2023-34046, CVE-2023-34051, CVE-2023-34052) |
| Description | VMwae has released security updates to address multiple vulnerabilities in their products. Exploitation of these vulnerabilities may lead to Privilege escalation, Information disclosure, Authentication bypass and Deserialization of data.<br>VMware recommends to apply the necessary security fixes at your earliest to avoid issues. |
| Affected Products | Workstation 17.x<br>Fusion 13.x<br>Fusion 13.x<br>VMware Aria Operations for Logs 8.x<br>VMware Cloud Foundation (VMware Aria Operations for Logs) 5.x, 4.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.vmware.com/security/advisories/VMSA-2023-0022.html<br>https://www.vmware.com/security/advisories/VMSA-2023-0021.html |

| | |
|---|---|
| Affected Product | **Qnap** |
| Severity | **High** |
| Affected Vulnerability | OS Command Injection Vulnerability (CVE-2023-23373) |
| Description | Qnap has released a security update addressing an OS command injection vulnerability that exists in QUSBCam2. If exploited, the vulnerability could allow users to execute arbitrary commands via a network.<br>Qnap recommends to apply the necessary security fixes at your earliest to avoid issues. |
| Affected Products | QUSBCam2 2.0.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.qnap.com/en/security-advisory/qsa-23-43 |

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | **High**, **Medium**, **Low** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-4921, CVE-2023-4622, CVE-2023-42755, CVE-2023-31083, CVE-2023-34319, CVE-2023-4881, CVE-2023-3772, CVE-2023-4623, CVE-2023-0597, CVE-2023-42753, CVE-2023-1206, CVE-2023-42752, CVE-2023-4244, CVE-2023-5197, CVE-2023-42756) |
| Description | Ubuntu has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution.<br>Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Ubuntu 14.04<br>Ubuntu 20.04<br>Ubuntu 22.04 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-6440-2<br>https://ubuntu.com/security/notices/USN-6446-1 |

**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.**