# Advisory Alert

**Alert Number:** AAA20240111 **Date:** January 11, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **Critical** | Arbitrary File Upload Vulnerability |
| **Ivanti** | **Critical** | Multiple Vulnerabilities |
| **Juniper** | **High**, **Medium** | Multiple Vulnerabilities |
| **Cisco** | **Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Critical** |
| Affected Vulnerability | Arbitrary File Upload Vulnerability (CVE-2024-20272) |
| Description | Cisco has released a security update addressing Arbitrary File Upload Vulnerability that exist in Cisco Unity Connection Release.<br><br>**CVE-2024-20272-** A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to upload arbitrary files to an affected system and execute commands on the underlying operating system.<br><br>Cisco recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Cisco Unity Connection Release 12.5 and earlier<br>Cisco Unity Connection Release 14 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuc-unauth-afu-FROYsCsD |

| | |
|---|---|
| Affected Product | **Ivanti** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2023-46805, CVE-2024-21887) |
| Description | Ivanti has released a security update addressing Authentication Bypass and Command Injection vulnerabilities that exists in Ivanti Connect Secure and Ivanti Policy Secure Gateways.<br><br>**CVE-2023-46805-** An authentication bypass vulnerability in the web component of Ivanti ICS 9.x, 22.x and Ivanti Policy Secure allows a remote attacker to access restricted resources by bypassing control checks.<br><br>**CVE-2024-21887-** A command injection vulnerability in web components of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an authenticated administrator to send specially crafted requests and execute arbitrary commands on the appliance.<br><br>Ivanti recommends to apply the necessary mitigations at your earliest to avoid issues. |
| Affected Products | Ivanti Connect Secure and Ivanti Policy Secure Gateways Version 9.x and 22.x |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US |

| | |
|---|---|
| Affected Product | **Juniper** |
| Severity | **High**, **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-21611, CVE-2024-21596) |
| Description | Juniper has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to denial of service.<br><br>**CVE-2024-21611 -** A Missing Release of Memory after Effective Lifetime vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause a Denial of Service when jflow is configured to [ services flow-monitoring (version-ipfix\|version9) ]<br><br>**CVE-2024-21596 -** A Heap-based Buffer Overflow vulnerability in the Routing Protocol Daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service which affects devices with NSR enabled.<br><br>It is recommended by Juniper to apply necessary security fixes at earliest to avoid issues |
| .Affected Products | jflow or non-stop routing (NSR) configuration enabled<br>Junos OS<br>Junos OS Evolved |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-In-a-jflow-scenario-continuous-route-churn-will-cause-a-memory-leak-and-eventually-an-rpd-crash-CVE-2024-21611?language=en_US<br>https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-specific-BGP-UPDATE-message-will-cause-a-crash-in-the-backup-Routing-Engine-CVE-2024-21596?language=en_US https://www.fortiguard.com/psirt/FG-IR-23-408 |

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **Medium** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-20251, CVE-2024-20270, CVE-2023-20257, CVE-2023-20258, CVE-2023-20260, CVE-2023-20271, CVE-2024-20287, CVE-2024-20277, CVE-2023-20248, CVE-2023-20249) |
| Description | Cisco has released security updates addressing multiple vulnerabilities that exists in their products. By exploiting these vulnerabilities could lead to Cross-Site Scripting, arbitrary commands execution, SQL injection, privileges escalation and Command Injection<br><br>It is recommended by Cisco to apply necessary security fixes at earliest to avoid issues |
| .Affected Products | Cisco TMS Software Release Earlier than 15.13.2<br>Cisco ThousandEyes Enterprise Agent Release 0.233 and earlier<br>Cisco WAP371 Wireless-AC/N Dual Radio AP with Single Point Setup<br>Cisco EPNM Release 7.0 and earlier,7.1<br>Cisco Prime Infrastructure Release3.9 and earlier ,3.10<br>Cisco BroadWorks BWCallCenter Earlier than 23.0, 24.0, 25.0<br>Cisco BroadWorks BWReceptionist Earlier than 23.0, 23.0, 24.0, 25.0<br>Cisco ISE Release 2.7 and earlier, 3.0, 3.1, 3.3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-XSS-bL4VTML<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-xss-6syj82Ju<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-wkZJeyeq<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-bHStWgXO<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-thouseyes-privesc-DmzHG3Qv<br>https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-portal-xss-AXNeVg3s |

**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.**