# Advisory Alert

**Alert Number:** AAA20240805 **Date:** August 5, 2024

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Cisco** | **High** | Remote Unauthenticated Code Execution Vulnerability |
| **SUSE** | **High** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Cisco** |
| Severity | **High** |
| Affected Vulnerability | Remote Unauthenticated Code Execution Vulnerability (CVE-2024-6387) |
| Description | Cisco has released security updates addressing a Remote Unauthenticated Code Execution Vulnerability that exists in the OpenSSH third-party product that in turn affects Cisco products.<br>**CVE-2024-6387** - A signal handler race condition was found in sshd, where a client does not authenticate within LoginGraceTime seconds (120 by default, 600 in old OpenSSH versions), then the sshd SIGALRM handler is called asynchronously. However, this signal handler calls various functions that are not async-signal-safe, for example, syslog().<br>Cisco advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | Network and Content Security Devices<br>• Adaptive Security Appliance (ASA) Software Prior to 9.18.4.34, 9.20.3<br>• Firepower Threat Defense (FTD) Software Prior to 7.4.2<br>• Identity Services Engine (ISE) Prior to 3.3 patch, 3.2 patch, 3.1 patch<br>Network Management and Provisioning<br>• Cyber Vision Prior to 4.1.7, 4.4.3, 5.0.0<br>• Prime Infrastructure Prior to 3.10.5<br>Routing and Switching - Enterprise and Service Provider<br>• 8000 Series Routers Prior to 24.2.11 SMU ID AA35431<br>• IOS XRd Control Plane Prior to 24.2.11 SMU ID AA35431<br>• IOS XRd vRouter Prior to 24.2.11 SMU ID AA35431<br>• Network Convergence System 540 Series Routers running NCS540L images Prior to 24.2.11 SMU ID AA35431<br>• Network Convergence System 1010 Prior to 24.2.11 SMU ID AA35431<br>• Network Convergence System 1014 Prior to 24.2.11 SMU ID AA35431<br>• Network Convergence System 5700 Fixed Chassis NCS-57B1, NCS-57C1, and NCS-57D2 Prior to 24.2.11 SMU ID AA35431<br>Unified Computing<br>• Intersight Virtual Appliance Prior to 1.0.9-677<br>Video, Streaming, TelePresence, and Transcoding Devices<br>• Board Series Prior to Cloud - RoomOS 11.18.1.6, On-premise - RoomOS 11.17.3.0, On-premise - RoomOS 11.14.4<br>• Desk Series Prior to Cloud - RoomOS 11.18.1.6, On-premise - RoomOS 11.17.3.0, On-premise - RoomOS 11.14.4<br>• Expressway Series Prior to X15.0.3<br>• Room Series Prior to Cloud - RoomOS 11.18.1.6, On-premise - RoomOS 11.17.3.0, On-premise - RoomOS 11.14.4<br>• TelePresence Video Communication Server (VCS) Prior to X15.0.3<br>• Webex Board Prior to Cloud - RoomOS 11.18.1.6, On-premise - RoomOS 11.17.3.0, On-premise - RoomOS 11.14.4<br>Wireless<br>• 6300 Series Embedded Services Access Points Prior to 17.12.4<br>• Aironet 802.11ac Wave2 Access Points Prior to 17.12.4<br>• Aironet 1540 Series Prior to 17.12.4<br>• Aironet 1560 Series Prior to 17.12.4<br>• Catalyst 9100 Series Access Points Prior to 17.12.4<br>• Catalyst IW6300 Heavy Duty Series Access Points Prior to 17.12.4<br>• Catalyst IW9165 Heavy Duty Series Prior to 17.12.4<br>• Catalyst IW9165 Rugged Series Prior to 17.12.4<br>• Catalyst IW9167 Heavy Duty Series Prior to 17.12.4 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssh-rce-2024 |

| | |
|---|---|
| Affected Product | **SUSE** |
| Severity | **High** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2024-27398, CVE-2024-35950, CVE-2022-48651, CVE-2023-52340, CVE-2023-52502, CVE-2023-6546, CVE-2024-23307, CVE-2024-26585, CVE-2024-26610, CVE-2024-26622, CVE-2024-26766, CVE-2024-26828, CVE-2024-26852, CVE-2024-26923, CVE-2024-26930) |
| Description | Suse 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, Local Privilege Escalation, Memory Corruption, Integer Overflow .<br>Suse advises to apply security fixes at your earliest to protect systems from potential threats. |
| Affected Products | OpenSUSE Leap 15.5<br>SUSE Linux Enterprise High Performance Computing 15 SP5<br>SUSE Linux Enterprise Live Patching 15-SP5<br>SUSE Linux Enterprise Micro 5.5<br>SUSE Linux Enterprise Real Time 15 SP5<br>SUSE Linux Enterprise Server 15 SP5<br>SUSE Linux Enterprise Server for SAP Applications 15 SP5 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | • https://www.suse.com/support/update/announcement/2024/suse-su-20242719-1<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20242722-1<br>• https://www.suse.com/support/update/announcement/2024/suse-su-20242723-1 |

**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.**