Advisory Alert

Alert Number: AAA20240808 **Date:** August 8, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**High**	Race Condition Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Hitachi	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20450, CVE-2024-20451, CVE-2024-20452 ,CVE-2024-20453, CVE-2024-20454)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to Execute Arbitrary Commands, Denial of Service. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All software releases that run on Cisco Small Business SPA300 Series and Cisco Small Business SPA500 Series IP Phones
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-spa-http-vulns-RJZmX2Xz

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Race Condition Vulnerability (CVE-2024-6387)
Description	IBM has released security updates addressing a Race Condition Vulnerability that exists in their products. **CVE-2024-6387 -** OpenSSH could allow a remote attacker to execute arbitrary code on the system, caused by a signal handler race condition. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code with root privileges on glibc-based Linux systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data – Version 5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7163719

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use after free conditions, Memory Corruption, NULL Dereference, Out of Bounds Read. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP6 Development Tools Module 15-SP6 Legacy Module 15-SP6 OpenSUSE Leap 15.3, 15.6 SUSE Linux Enterprise Desktop 15 SP6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP3 SUSE Linux Enterprise Live Patching 15-SP3 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Server 15 SP3 SUSE Linux Enterprise Server for SAP Applications 15 SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20242802-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20242815-1/

Affected Product	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21417, CVE-2024-28899, CVE-2024-30013, CVE-2024-30071, CVE-2024-30079, CVE-2024-30081, CVE-2024-30098, CVE-2024-35270, CVE-2024-3596, CVE-2024-37969, CVE-2024-37970, CVE-2024-37971, CVE-2024-37972, CVE-2024-37973, CVE-2024-37974, CVE-2024-37975, CVE-2024-37981, CVE-2024-37984, CVE-2024-37986, CVE-2024-37987, CVE-2024-37988, CVE-2024-37989, CVE-2024-38010, CVE-2024-38011, CVE-2024-38013, CVE-2024-38017, CVE-2024-38019, CVE-2024-38022, CVE-2024-38025, CVE-2024-38027, CVE-2024-38028, CVE-2024-38030, CVE-2024-38032, CVE-2024-38033, CVE-2024-38034, CVE-2024-38041, CVE-2024-38043, CVE-2024-38047, CVE-2024-38048, CVE-2024-38049, CVE-2024-38050, CVE-2024-38051, CVE-2024-38052, CVE-2024-38053, CVE-2024-38054, CVE-2024-38055, CVE-2024-38056, CVE-2024-38057, CVE-2024-38058, CVE-2024-38059, CVE-2024-38060, CVE-2024-38061, CVE-2024-38062, CVE-2024-38064, CVE-2024-38065, CVE-2024-38066, CVE-2024-38068, CVE-2024-38069, CVE-2024-38070, CVE-2024-38079, CVE-2024-38081, CVE-2024-38085, CVE-2024-38091, CVE-2024-38101, CVE-2024-38102, CVE-2024-38104, CVE-2024-38105, CVE-2024-38112, CVE-2024-38517, CVE-2024-39684)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Remote Code Execution, Information Disclosure, Denial of Service. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H Hitachi Virtual Storage Platform G1000, G1500 Hitachi Virtual Storage Platform F1500 Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/07.html

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20236, CVE-2024-20443, CVE-2024-20479)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use after free conditions, Memory corruption, Integer Overflow or Wraparound, out-of-bounds read. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE Release 3.0 - 3.3 and prior to 2.7 8000 Series Routers prior to 7.10.1 ASR 9000 Series Lightspeed-based line cards prior to 24.1.1 ASR 9901 prior to 24.3.1 ASR 9903 prior to 24.3.1 NCS 560 prior to 24.2.1 NCS 1004 prior to 24.1.1 NCS 5500 prior to 7.10.1 NCS 5700 prior to 7.10.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ipxe-sigbypass-pymfyqgB • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-V2bm9JCY

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.