Advisory Alert

Alert Number: **AAA20240502** **Date:** **May 7, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Ubuntu	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26304, CVE-2024-26305, CVE-2024-33511, CVE-2024-33512, CVE-2024-33513, CVE-2024-33514, CVE-2024-33515, CVE-2024-33516, CVE-2024-33517, CVE-2024-33518)
Description	HPE has issued security updates addressing multiple vulnerabilities that exist in HPE products. If Exploited, these vulnerabilities could lead to Arbitrary Code Execution, Denial of Service (DoS). HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking • Mobility Conductor (formerly Mobility Master) • Mobility Controllers • WLAN Gateways and SD-WAN Gateways managed by Aruba Central Affected Software Versions • ArubaOS 10.5.x.x: 10.5.1.0 and below • ArubaOS 10.4.x.x: 10.4.1.0 and below • ArubaOS 8.11.x.x: 8.11.2.1 and below • ArubaOS 8.10.x.x: 8.10.0.10 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04640en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-51385, CVE-2023-45871)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM products. **CVE-2023-51385** - OpenSSH could allow a remote attacker to execute arbitrary commands on the system, caused by improper validation of shell metacharacters. By sending a specially crafted request using expansion tokens, an attacker could exploit this vulnerability to execute arbitrary commands on the system. **CVE-2023-45871** - Linux Kernel is vulnerable to a buffer overflow, caused by improper bounds checking by the IGB driver in drivers/net/ethernet/intel/igb/igb_main.c. By sending a specially crafted request, a remote attacker could overflow a buffer and execute arbitrary code or cause a denial of service condition on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Copy Data Management 2.2.0.0 - 2.2.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145938 • https://www.ibm.com/support/pages/node/7145939

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20357, CVE-2024-20376, CVE-2024-20378)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in Cisco IP Phones. **CVE-2024-20357** - A vulnerability in the XML service of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to initiate phone calls on an affected device. This vulnerability exists because bounds-checking does not occur while parsing XML requests. **CVE-2024-20376** - A vulnerability in the web-based management interface of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a DoS condition. This vulnerability is due to insufficient validation of user-supplied input. **CVE-2024-20378** - A vulnerability in the web-based management interface of Cisco IP Phone firmware could allow an unauthenticated, remote attacker to retrieve sensitive information from an affected device. This vulnerability is due to a lack of authentication for specific endpoints of the web-based management interface on an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IP Phone 6800, 7800, and 8800 - Cisco Multiplatform Firmware Release 12.0.4 and earlier Video Phone 8875 - Cisco PhoneOS 2.3.1.001 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipphone-multi-vulns-cXAhCvS

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. If Exploited, these vulnerabilities could lead to Memory leakage, NULL pointer dereferences, Use after free conditions. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 SUSE Linux Enterprise Desktop 15 SP5 SUSE Linux Enterprise High Availability Extension 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241480-1/

Affected Product	**Ubuntu**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0193, CVE-2024-26597, CVE-2023-51781, CVE-2023-6817, CVE-2023-4569, CVE-2024-1085, CVE-2024-1086)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of service, Arbitrary code execution and Sensitive information disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0103-1

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Memory exhaustion, NULL pointer dereferences, Improper access control. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8, 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8, 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8, 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8, 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8, 9.2 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8, 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV 9 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8, 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4, 8.8, 9.2 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 8.4, 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.4, 8.8 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4, 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:2628 • https://access.redhat.com/errata/RHSA-2024:2627 • https://access.redhat.com/errata/RHSA-2024:2621 • https://access.redhat.com/errata/RHSA-2024:2585 • https://access.redhat.com/errata/RHSA-2024:2582 • https://access.redhat.com/errata/RHSA-2024:2394

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28775, CVE-2024-26308, CVE-2024-25710, CVE-2024-0985, CVE-2024-29131, CVE-2024-29133, CVE-2024-28764, CVE-2023-48795, CVE-2023-2166, CVE-2023-40283, CVE-2023-1838, CVE-2023-5717, CVE-2023-6817, CVE-2024-0646, CVE-2023-6606, CVE-2023-46813, CVE-2023-4921, CVE-2023-6536, CVE-2023-4623, CVE-2023-6356, CVE-2023-2269, CVE-2023-6610, CVE-2023-6535)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege escalation, Denial of service, Internal information disclosure, Arbitrary command execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Automation 1.7.0 IBM Storage Copy Data Management 2.2.0.0 - 2.2.23.0 IBM WebSphere Extreme Scale 8.6.1.0 - 8.6.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7149856 • https://www.ibm.com/support/pages/node/7145940 • https://www.ibm.com/support/pages/node/7150045 • https://www.ibm.com/support/pages/node/7149857 • https://www.ibm.com/support/pages/node/7145939

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.