Advisory Alert

Alert Number: AAA20240404 **Date:** April 4, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
NodeJS	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
Ivanti	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-44906, CVE-2024-28176, CVE-2023-42282. CVE-2024-28849 CVE-2023-51775, CVE-2023-6378, CVE-2024-22257, CVE-2024-22259)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service, Remote Authentication Bypass and Information disclosure. HPE recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Unified OSS Console (UOC) - Prior to v3.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04629en_us

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0461, CVE-2023-39191, CVE-2023-46813, CVE-2023-51779, CVE-2023-6531)
Description	Suse has released security updates addressing multiple vulnerabilities that exist in their Linux Kernel RT. Exploitation of these vulnerabilities could lead to Use-after-free, Arbitrary code execution, Privilege escalation. Suse recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.5 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20241097-1

Affected Product	**NodeJS**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27983, CVE-2024-27982)
Description	NodeJS has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to HTTP request smuggling and HTTP/2 server crash. NodeJS recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NodeJS - Versions 18.x, 20.x, 21.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/april-2024-security-releases

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-6176, CVE-2023-4569, CVE-2024-0646, CVE-2024-1086, CVE-2023-51781, CVE-2023-1872)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their Linux kernel. Exploitation of these vulnerabilities could lead to Use-after-free, Denial of service, Arbitrary code execution, expose sensitive information. Ubuntu recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/LSN-0102-1

Affected Product	**Ivanti**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, CVE-2024-22023)
Description	Ivanti has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Heap overflow, Denial of service, Execute arbitrary code, Null pointer dereference. Ivanti recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti Connect Secure (ICS) - Version 9.x and 22.x Ivanti Policy Secure
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/SA-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20347, CVE-2024-20352, CVE-2024-20310, CVE-2024-20367 CVE-2024-20368, CVE-2024-20332, CVE-2024-20281, CVE-2024-20283, CVE-2024-20302 CVE-2024-20282, CVE-2024-20362, CVE-2024-20334, CVE-2024-20348)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Arbitrary code execution, Exposure sensitive information, Cross-Site Request Forgery, Directory Traversal. Cisco recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Emergency Responder Release 14, 12.5(1) and earlier Cisco Unified CM IM&P Release 14, 12.5(1) and earlier Cisco ECE Software Release 12.5, 12.6 Cisco ISE Release 3.0 to 3.3, 2.7 and earlier Cisco Nexus Dashboard Release 3.0, 3.1, 2.3 and earlier Cisco NDFC Release 12.0 and 12.1.3 Cisco NDI Release 6.4, 6.3, 6.2 and earlier Cisco NDO Release 4.3, 4.2, 4.1 and earlier Cisco RV016 Multi-WAN VPN Routers Cisco RV042 Dual WAN VPN Routers Cisco RV042G Dual Gigabit WAN VPN Routers Cisco RV082 Dual WAN VPN Routers Cisco RV320 Dual Gigabit WAN VPN Routers Cisco RV325 Dual Gigabit WAN VPN Routers Cisco TMS Software Release Earlier than 15.13.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cem-csrf-suCmNjFr • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-imps-xss-quWkd9yF • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ece-xss-CSQxgxfM • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-NfAKXrp5 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-ssrf-FtSTh5Oz • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfccsrf-TEmZEfJ9 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndidv-LmXdvAf2 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndo-upav-YRqsCcSP • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndru-pesc-kZ2PQLZH • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbiz-rv-xss-OQeRTup • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-tms-xss-kGw4DX9Y • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-dir-trav-SSn3AYDw

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33631, CVE-2023-1118, CVE-2024-26602)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Use-after-free, Integer overflow. Red Hat recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat Virtualization Host 4 for RHEL 8 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.6 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.6 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1653

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27268, CVE-2024-27270, CVE-2024-22353, CVE-2023-50313)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Use-after-free. Denial of service and Cross-site scripting IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Liberty - Version 17.0.0.3 - 24.0.0.3 IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Application Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145809 • https://www.ibm.com/support/pages/node/7145836 • https://www.ibm.com/support/pages/node/7145835 • https://www.ibm.com/support/pages/node/7145880 • https://www.ibm.com/support/pages/node/7145833 • https://www.ibm.com/support/pages/node/7145807 • https://www.ibm.com/support/pages/node/7145878

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.