Advisory Alert

Alert Number: AAA20240516 **Date:** May 17, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Access Bypass Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Dell	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Intel	**Medium**	Insecure De-synchronization Vulnerability

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has issued security updates addressing an Access Bypass Vulnerability that exists in RESTful Web Services. This module exposes Drupal resources (e.g. entities) as RESTful web services. The module doesn't sufficiently restrict access for user resources. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	RESTful Web Services module for Drupal 7 versions below 2.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-019

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-23307, CVE-2020-9493, CVE-2019-17571, CVE-2024-1597)
Description	IBM has issued security updates addressing multiple vulnerabilities that exist in IBM QRadar SIEM. These vulnerabilities could be exploited by remote attackers to cause SQL Injection and Execute Arbitrary Code on the system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7152257 • https://www.ibm.com/support/pages/node/7152260

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in SUSE Linux kernel. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Filesystem Corruption, Information Disclosure, 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 SP2, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP2, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Live Patching 15-SP2, 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP2, 15 SP5 SUSE Linux Enterprise Server 15 SP2 Business Critical Linux 15-SP2 SUSE Linux Enterprise Server 15 SP2 LTSS 15-SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2, 15 SP5 SUSE Linux Enterprise Workstation Extension 15 SP5 SUSE Manager Proxy 4.1 SUSE Manager Retail Branch Server 4.1 SUSE Manager Server 4.1 SUSE Real Time Module 15-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20241663-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241659-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20241650-1/

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2021-38575)
Description	HPE 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, Buffer Overflow, Remote Code Execution, and gain Local Unauthorized Access. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to v2.16_03-01-2024 HPE Alletra 4120 - Prior to v2.16_03-01-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE Apollo 2000 System - Prior to v3.10_02-22-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE Compute Edge Server e930t - Prior to v2.16_03-01-2024 HPE Edgeline e920 Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920d Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920t Server Blade - Prior to v2.00_02-22-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant DL110 Gen10 Plus Telco server - Prior to v2.00_02-22-2024 HPE ProLiant DL110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL320 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL360 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL380 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant DL380a Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL560 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant DX170r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX190r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX220n Gen10 Plus server - Prior to v2.00_02-22-2024 HPE ProLiant DX360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX360 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX380 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX4200 Gen10 server - Prior to v2.00_02-22-2024 HPE ProLiant DX560 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant e910 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant e910t Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML110 Gen11 - Prior to v2.16_03-01-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML350 Gen11 Server - Prior to v2.16_03-01-2024 HPE ProLiant RL300 Gen11 - Prior to v1.60_03-07-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.00_02-22-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.16_03-01-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.10_02-22-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04593en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22429, CVE-2023-32460, CVE-2023-48795, CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20922, CVE-2024-20923, CVE-2024-20925, CVE-2024-20926, CVE-2024-20932, CVE-2024-20945, CVE-2024-20952, CVE-2023-45745, CVE-2023-47855, CVE-2023-45733, CVE-2023-28402, CVE-2023-27504, CVE-2023-28383, CVE-2024-21828)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000221102/dsa-2024-020 • https://www.dell.com/support/kbdoc/en-us/000225071/dsa-2024-140-security-update-for-dell-disk-library-for-mainframe-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225088/dsa-2024-192-security-update-for-data-protection-advisor-and-powerprotect-dp-series-appliance-idpa-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000224980/dsa-2024-206-dell-poweredge-server-security-update-for-intel-ethernet-controllers-adapters-vulnerability • https://www.dell.com/support/kbdoc/en-us/000224981/dsa-2024-160-security-update-for-dell-poweredge-server-for-intel-may-2024-security-advisories-2024-2-ipu • https://www.dell.com/support/kbdoc/en-us/000219969/dsa-2023-449 • https://www.dell.com/support/kbdoc/en-us/000224971/dsa-2024-216-security-update-for-dell-precision-rack-for-intel-ethernet-controller-administrative-tools-installer-software-vulnerabilities

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20326, CVE-2024-20389, CVE-2024-20366, CVE-2024-20391, CVE-2024-20369, CVE-2024-20256, CVE-2024-20257, CVE-2024-20258, CVE-2024-20383, CVE-2024-20392, CVE-2024-20394)
Description	Cisco 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, Privilege Escalation, Cross-Site Scripting, read and write arbitrary files. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Crosswork NSO Releases • Versions 5.1.7, 5.2.7, 5.3.5, 5.4.5 • 5.5.3 – versions below 5.5.10.1 • 5.6 – versions below 5.6.14.3 • 5.7 – versions below 5.7.15 • 5.8 – versions below 5.8.13.1 • 6.0 – versions below 6.0.12 • 6.1 – versions below 6.1.7 • 6.2 – versions below 6.2.2 • Versions below 5.0 and 6.0 if they are running on Tail-f HCC function pack versions below 5.0.5 and 6.0.2 ConfD Release • Versions 7.1.7, 7.2.7, 7.3.5, 7.4.5 • 7.5.3 – versions below 7.5.10.2 • 7.6 – versions below 7.6.14.2 • 7.7 – versions below 7.7.15 • 7.8 – versions below 7.8.13.1 • 8.0 – versions below 8.0.12 Secure Email and Web Manager using Cisco AsyncOS interface Releases prior to 15.5.1 Secure Email Gateway using Cisco AsyncOS interface Releases prior to 15.5.1-055 Secure Web Appliance using Cisco AsyncOS interface Releases prior to 14.5.2-011 and 15.0.0-355 Cisco AppDynamics Network Visibility Agent versions prior to 24.4.0 Cisco Secure Client Releases prior to 5.1.3.62
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnfd-rwpesc-ZAOufyx8 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-rwpesc-qrQGnh3f • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-hcc-priv-esc-OWBWCs5D • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-secure-nam-priv-esc-szu2vYpZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nso-ordir-MNM8YqzO • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-wsa-xss-bgG5WHOD • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appd-netvisdos-9zNbsJtK • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-http-split-GLrnnOwS

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-26464, CVE-2022-23302, CVE-2020-9488, CVE-2022-23305, CVE-2021-4104, CVE-2023-46158, CVE-2023-44487, CVE-2023-31582, CVE-2023-51775)
Description	IBM 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, Sensitive Information Disclosure, Arbitrary Code Execution. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP8 IBM Elastic Storage Server versions 6.1.0.0 - 6.1.2.8 and versions 6.1.3.0 - 6.1.9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7152257 • https://www.ibm.com/support/pages/node/7152258 • https://www.ibm.com/support/pages/node/7152275

Affected Product	**Intel**
Severity	**Medium**
Affected Vulnerability	Insecure De-synchronization Vulnerability (CVE-2024-21823)
Description	Intel has released security updates addressing an Insecure De-synchronization Vulnerability that exists in Intel Xeon processors. **CVE-2024-21823** - Hardware logic with insecure de-synchronization in Intel DSA and Intel IAA for some Intel 4th or 5th generation Xeon processors may allow an authorized user to potentially enable denial of service via local access. Intel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	**DSA version 1.0 and IAA version 1.0 on below processors** • 5th Generation Intel Xeon Scalable processors • 4th Generation Intel Xeon Scalable processors • 4th Generation Intel Xeon Platinum processors • 4th Generation Intel Xeon Gold Processors • 4th Generation Intel Xeon Silver Processors • 4th Generation Intel Xeon Bronze Processors • 4th Gen Intel Xeon Scalable Processors with Intel® vRAN • Intel® Xeon® W workstation processors
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01084.html

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.