Advisory Alert

Alert Number: AAA20240829 **Date:** August 29, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**	Denial of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Access bypass Vulnerability
Dell	**Medium** , **Low**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31315, CVE-2023-52771, CVE-2023-52880, CVE-2024-26581, CVE-2024-26668, CVE-2024-26810, CVE-2024-26855, CVE-2024-26908, CVE-2024-26925, CVE-2024-27016, CVE-2024-27019, CVE-2024-27020, CVE-2024-27415, CVE-2024-35839, CVE-2024-35896, CVE-2024-35897, CVE-2024-35898, CVE-2024-35962, CVE-2024-36003, CVE-2024-36025, CVE-2024-38538, CVE-2024-38540, CVE-2024-38544, CVE-2024-38579, CVE-2024-38608, CVE-2024-39476, CVE-2024-40905, CVE-2024-40911, CVE-2024-40912, CVE-2024-40914, CVE-2024-40929, CVE-2024-40939, CVE-2024-40941, CVE-2024-40957, CVE-2024-40978, CVE-2024-40983, CVE-2024-41041, CVE-2024-41076, CVE-2024-41090, CVE-2024-41091, CVE-2024-42110, CVE-2024-42152)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause SMM Lock Bypass, NULL pointer dereference, denial of service, memory leak. 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 9.4 aarch64 Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Real Time 9 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 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) 7 s390x Red Hat Enterprise Linux Server - Extended Life Cycle Support 7 x86_64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian 7 ppc64 Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian 7 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:5982 • https://access.redhat.com/errata/RHSA-2024:5980 • https://access.redhat.com/errata/RHSA-2024:5978 • https://access.redhat.com/errata/RHSA-2024:5928

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-50308)
Description	IBM has released security update addressing a Denial of Service Vulnerability that exists in IBM Db2. **CVE-2024-38304-** IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) under certain circumstances could allow an authenticated user to the database to cause a denial of service when a statement is run on columnar tables. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server 11.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7105506

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-52772, CVE-2024-36921)
Description	SUSE 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. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20243060-1/

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20279, CVE-2024-20478, CVE-2024-20411, CVE-2024-20413, CVE-2024-20289, CVE-2024-20284, CVE-2024-20285, CVE-2024-20286, CVE-2024-20446)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of service, Privilege Escalation, Arbitrary Code Execution, Command Injection. Cisco 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://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cousmo-uBpBYGbq • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-priv-esc-uYQJjnuU • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-bshacepe-bApeHSx7 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cmdinj-Lq6jsZhH • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-psbe-ce-YvbTn5du • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvis ory/cisco-sa-nxos-dhcp6-relay-dos-znEAA6xn

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access bypass Vulnerability
Description	Drupal has released security updates addressing an Access bypass Vulnerability that exists in advanced varnish module. The Varnish bin names may be guessable when no hashing noise configuration is set on the module configuration page, which would ultimately allow any user to view cached pages that were intended for other roles when guessing such a bin name. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Advanced Varnish module for Drupal 4.0.x before 4.0.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-033

Affected Product	**Dell**
Severity	**Medium** , **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38303, CVE-2024-38304)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-38303-** Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Improper Input Validation vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. **CVE-2024-38304-** Dell PowerEdge Platform, 14G Intel BIOS version(s) prior to 2.22.x, contains an Access of Memory Location After End of Buffer vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC Storage NX3240 BIOS Versions prior to 2.22.1 Dell EMC Storage NX3340 BIOS Versions prior to 2.22.1 Dell EMC XC Core 6420 System BIOS Versions prior to 2.22.0 Dell EMC XC Core XC640 System BIOS Versions prior to 2.22.1 Dell EMC XC Core XC740xd System BIOS Versions prior to 2.22.1 Dell EMC XC Core XC740xd2 BIOS Versions prior to 2.22.0 Dell EMC XC Core XC940 System BIOS Versions prior to 2.22.1 Dell EMC XC Core XCXR2 BIOS Versions prior to 2.22.0 DSS 8440 BIOS Versions prior to 2.22.0 PowerEdge C4140 BIOS Versions prior to 2.22.0 PowerEdge C6420 BIOS Versions prior to 2.22.0 PowerEdge FC640 BIOS Versions prior to 2.22.0 PowerEdge M640 BIOS Versions prior to 2.22.0 PowerEdge M640 (for PE VRTX) BIOS Versions prior to 2.22.0 PowerEdge MX740C BIOS Versions prior to 2.22.0 PowerEdge MX840C BIOS Versions prior to 2.22.0 PowerEdge R440 BIOS Versions prior to 2.22.0 PowerEdge R540 BIOS Versions prior to 2.22.0 PowerEdge R640 BIOS Versions prior to 2.22.1 PowerEdge R740 BIOS Versions prior to 2.22.1 PowerEdge R740XD BIOS Versions prior to 2.22.1 PowerEdge R740XD2 BIOS Versions prior to 2.22.0 PowerEdge R840 BIOS Versions prior to 2.22.0 PowerEdge R940 BIOS Versions prior to 2.22.1 PowerEdge R940XA BIOS Versions prior to 2.22.0 PowerEdge T440 BIOS Versions prior to 2.22.0 PowerEdge T640 BIOS Versions prior to 2.22.0 PowerEdge XE2420 BIOS Versions prior to 2.22.0 PowerEdge XE7420 BIOS Versions prior to 2.22.0 PowerEdge XE7440 BIOS Versions prior to 2.22.0 PowerEdge XR2 BIOS Versions prior to 2.22.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000228137/dsa-2024-310-security-update-for-dell-poweredge-server-for-access-of-memory-location-after-end-of-buffer-vulnerability • https://www.dell.com/support/kbdoc/en-us/000228135/dsa-2024-309-security-update-for-dell-poweredge-server-for-improper-input-validation-vulnerability

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.