TLP: WHITE

Advisory Alert

Alert Number: AAA20240229 **Date:** February 29, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
IBM	Medium	Security Update
Drupal	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39198, CVE-2023-4921, CVE-2023-51780, CVE-2023-1829)
Description	Suse has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Use-after-free condition and Race condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP2 SUSE Linux Enterprise Live Patching 15-SP2 SUSE Linux Enterprise Server 15 SP2 SUSE Linux Enterprise Server for SAP Applications 15 SP2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240655-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240656-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240665-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240663-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240662-1/

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38096, CVE-2023-4244, CVE-2023-6546, CVE-2023-6817, CVE-2023-6931, CVE-2023-51042, CVE-2023-51043, CVE-2024-0193, CVE-2024-1085, CVE-2024-1086)
Description	Red Hat has released security updates addressing multiple vulnerabilities. An attacker may exploit these vulnerabilities to cause Out of boundary writes, Use-after-free, NULL pointer dereference, Privilege escalation. Red Hat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 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 for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:1018 https://access.redhat.com/errata/RHSA-2024:1019

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-32460, 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-2023-20592, CVE-2023-39432, CVE-2023-33870)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third-party components that in turn affect dell products. Exploitation of these vulnerabilities could lead to Privilege escalation, Denial of service, Unauthorized access, Sensitive information disclosure Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VxFlex Ready Node • Dell PowerEdge BIOS- 14G R640, R740, R840 Versions prior to 2.20.1 PowerFlex Custom Node • Dell PowerEdge BIOS –15G R650 and R750 Versions prior to 1.12.1 • Dell PowerEdge BIOS –15G AMD R6525 and R7525 Versions prior to 2.13.3 • Dell PowerEdge BIOS –16G R660 and R760 Versions prior to 1.6.6 • Dell PowerEdge BIOS –16G AMD R6625 and R7625 Versions prior to 1.6.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222598/dsa-2024-101-security-update-for-dell-vxflex-ready-node-and-powerflex-custom-node-multiple-third-party-component-vulnerabilities

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20321, CVE-2024-20267, CVE-2024-20344, CVE-2024-20291, CVE-2024-20294)
Description	Cisco has released a security update addressing multiple vulnerabilities that exist in their products. An attacker may exploit these vulnerabilities to cause Denial of service and Unauthorized access, Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Nexus 3600 Series Switches and Cisco Nexus 9500 R-Series Line Cards • N3K-C36180YC-R • N3K-C3636C-R • N9K-X9624D-R2 • N9K-X9636C-R • N9K-X9636C-RX • N9K-X9636Q-R • N9K-X96136YC-R Nexus 3000 Series Switches (CSCwh42690) Nexus 5500 Platform Switches (CSCva52387) Nexus 5600 Platform Switches (CSCva52387) Nexus 6000 Series Switches (CSCva52387) Nexus 7000 Series Switches (CSCva52387) Cisco IMM Management Package Release 1.0.11 and earlier Cisco Nexus 3000 and 9000 Series Switches in standalone NX-OS mode if they were running Cisco NX-OS Software Release 9.3(10), 9.3(11), or 9.3(12) Cisco FXOS or NX-OS Software and had the LLDP feature enabled globally and on at least one interface: • Firepower 4100 Series (CSCwi29934) • Firepower 9300 Security Appliances (CSCwi29934) • MDS 9000 Series Multilayer Switches (CSCwf67408) • Nexus 3000 Series Switches (CSCwe86457) • Nexus 5500 Platform Switches (CSCwf67411) • Nexus 5600 Platform Switches (CSCwf67411) • Nexus 6000 Series Switches (CSCwf67411) • Nexus 7000 Series Switches (CSCwf67409) • Nexus 9000 Series Fabric Switches in ACI mode (CSCwi31871) • Nexus 9000 Series Switches in standalone NX-OS mode (CSCwe86457) • UCS 6200 Series Fabric Interconnects (CSCwf67412) • UCS 6300 Series Fabric Interconnects (CSCwf67412) • UCS 6400 Series Fabric Interconnects (CSCwf67468) • UCS 6500 Series Fabric Interconnects (CSCwf67468)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-ebgp-dos-L3QCwVJ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-mpls-dos-R9ycXkwM https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsfi-imm-syn-p6kZTDQC https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-po-acl-TkyePgvL https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-lldp-dos-z7PncTgt

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0565, CVE-2024-0646, CVE-2023-6915, CVE-2024-0582, CVE-2023-51781, CVE-2023-51780)
Description	Ubuntu has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Denial of service, Arbitrary code execution and Sensitive information disclosure Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 23.10 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6651-2

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2023-50312)
Description	IBM has released a security update for IBM WebSphere Application Server Liberty because it could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM WebSphere Application Server Liberty 17.0.0.3 - 24.0.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7125527

Affected Product	**Drupal**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Drupal has released a security update addressing multiple vulnerabilities. Exploitation of these vulnerabilities could lead to Cross Site Scripting, Access bypass and Cross Site Request Forgery. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Coffee module less than 1.4.0 for Drupal 10 Private Content module less than 2.1.0 for Drupal 8.x Node_access_rebuild_progressive module less than 7.x-1.2 for Drupal 7 Drupal Symfony Mailer Lite less than 1.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-011 https://www.drupal.org/sa-contrib-2024-012 https://www.drupal.org/sa-contrib-2024-013 https://www.drupal.org/sa-contrib-2024-014

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.