TLP: WHITE

Advisory Alert

Alert Number: **AAA20240822** **Date:** **August 22, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium** , **Low**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities
Drupal	**Medium**	Access Bypass Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23583)
Description	Dell has released security updates to address a vulnerability in Intel processors that affects Dell products. **CVE-2023-23583** - Sequence of processor instructions leads to unexpected behavior for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege and/or information disclosure and/or denial of service via local access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerSwitch Z9664F-ON – Firmware Versions prior to v3.54.5.1-7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000227962/dsa-2024-366-security-update-for-powerswitch-z9664f-on-vulnerability

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2024-20375, CVE-2024-6387, CVE-2024-20417, CVE-2024-20466, CVE-2024-20486, CVE-2024-20488)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Blind SQL injection, Denial of Service, Information Disclosure, Unauthenticated Code Execution, Cross-Site Request Forgery and Cross-Site Scripting. 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-cucm-dos-kkHq43We • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssh-rce-2024 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rest-5bPKrNtZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-info-exp-vdF8Jbyk • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-y4ZUz5Rj • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-9zmfHyZ

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-30171, CVE-2024-30172, CVE-2024-29857)
Description	IBM has released security updates to address multiple vulnerabilities in the IBM Db2 federated server, which is affected by issues in the open-source bcprov-jdk18on library.These vulnerabilities could be exploited to cause denial of service, and sensitive information disclosure. **CVE-2024-30172 -** The Bouncy Castle Crypto Package For Java is vulnerable to a denial of service, caused by an infinite loop in the Ed25519 verification code. By persuading a victim to use a specially crafted signature and public key, a remote attacker could exploit this vulnerability to cause a denial of service condition. **CVE-2024-29857 -** The Bouncy Castle Crypto Package For Java is vulnerable to a denial of service, caused by improper input validation. By importing an EC certificate with crafted F2m parameters, a remote attacker could exploit this vulnerability to cause excessive CPU consumption **CVE-2024-30171 -** The Bouncy Castle Crypto Package For Java could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw in the RSA decryption (both PKCS#1v1.5 and OAEP) feature. By utilize timing side-channel attack techniques, an attacker could exploit this vulnerability to obtain sensitive information, and use this information to launch further attacks against the affected system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 11.5.0 - 11.5.9 on Linux
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7165340

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, NULL dereference, Security restriction Bypass. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 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/USN-6975-1 • https://ubuntu.com/security/notices/USN-6974-1 • https://ubuntu.com/security/notices/USN-6973-1 • https://ubuntu.com/security/notices/USN-6972-1 • https://ubuntu.com/security/notices/USN-6971-1 • https://ubuntu.com/security/notices/USN-6950-4 • https://ubuntu.com/security/notices/USN-6951-4

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47069, CVE-2021-47356, CVE-2021-47468, CVE-2022-48793, CVE-2022-48799, CVE-2023-52434, CVE-2023-52610, CVE-2023-52864, CVE-2024-35845, CVE-2024-36016, CVE-2024-36904, CVE-2024-36941, CVE-2024-38570)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:5692

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability
Description	Drupal has released security updates addressing an Access Bypass Vulnerability that exists in Drupal Responsive and off-canvas menu. This module integrates the mmenu library with Drupal's menu system to create an off-canvas mobile menu and a horizontal menu at wider widths, but it doesn't respect custom node access restrictions implemented through hook_ENTITY_TYPE_access hooks, meaning the titles of restricted nodes can appear in the menu. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	4.x branch of the responsive_menu module prior to 4.4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2024-030

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.