TLP: WHITE

Advisory Alert

Alert Number: **AAA20250515** **Date:** **May 15, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Node.js	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226, CVE-2024-38812, CVE-2024-38813)
Description	Dell has released a security update addressing multiple vulnerabilities in their products. If exploited, These vulnerabilities could be exploited by malicious users to compromise affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerFlex Appliance - IC - Versions prior to IC-38.367.01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000321268/dsa-2025-209-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53141, CVE-2025-21756)
Description	Red Hat has released a security update addressing multiple vulnerabilities in their products. **CVE-2024-53141 -** In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks. **CVE-2025-21756 -** A flaw was found in the Linux kernel's VMware network driver, where an improperly timed socket unbinding could result in a use-after-free issue. This flaw allows an attacker who can create and destroy arbitrary connections on virtual connections to read or modify system memory, potentially leading to an escalation of privileges or the compromise of sensitive data. 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-2025:7652

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-33104, CVE-2024-11168, CVE-2024-9287, CVE-2024-56201, CVE-2024-56326, CVE-2023-0286, CVE-2023-50782, CVE-2024-0727, CVE-2022-49043, CVE-2024-10963, CVE-2024-10041, CVE-2024-3651, CVE-2020-11023, CVE-2024-50602, CVE-2023-5752, CVE-2019-12900, CVE-2024-47072, CVE-2022-39135, CVE-2020-13955, CVE-2022-34169, CVE-2022-41678, CVE-2024-29131, CVE-2024-29133, CVE-2022-42003, CVE-2022-42004, CVE-2023-35116, VE-2023-50386, CVE-2023-50291, CVE-2023-50292, CVE-2023-50298, CVE-2024-55549, CVE-2025-24855)
Description	IBM has released security updates addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause Server-Side Request Forgery (SSRF), NULL Pointer Dereference, Use After Free and Out-of-bounds Write. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server Versions - 9.0, 8.5 IBM QRadar SIEM Versions - 7.5 - 7.5.0 UP11 IF04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7233438 • https://www.ibm.com/support/pages/node/7233394

Affected Product	**Node.js**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23166, CVE-2025-23167, CVE-2025-23165)
Description	Node.js has released security updates addressing multiple vulnerabilities in their products. **CVE-2025-23166 -** The C++ method SignTraits::DeriveBits() may incorrectly call ThrowException() based on user-supplied inputs when executing in a background thread, crashing the Node.js process. Such cryptographic operations are commonly applied to untrusted inputs. Thus, this mechanism potentially allows an adversary to remotely crash a Node.js runtime. **CVE-2025-23167 -** A flaw in Node.js 20's HTTP parser allows improper termination of HTTP/1 headers using \r\n\rX instead of the required \r\n\r\n. This inconsistency enables request smuggling, allowing attackers to bypass proxy-based access controls and submit unauthorized requests. **CVE-2025-23165 -** In Node.js, the ReadFileUtf8 internal binding leaks memory due to a corrupted pointer in uv_fs_s.file: a UTF-16 path buffer is allocated but subsequently overwritten when the file descriptor is set. This results in an unrecoverable memory leak on every call. Repeated use can cause unbounded memory growth, leading to a denial of service. Node.js advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NodeJS 20.x, 22.x, 23.x, 24.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/may-2025-security-releases#corrupted-pointer-in-nodefsreadfileutf8const-functioncallbackinfovalue-args-when-args0-is-a-string-cve-2025-23165---low

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48012, CVE-2025-48011, CVE-2025-48010, CVE-2025-48009, CVE-2025-4416, CVE-2025-4415)
Description	Drupal has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerability could be exploited by malicious users to cause Access bypass, Denial of Service, Cross Site Scripting. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal One Time Password Versions Prior to 1.3.0 Drupal Single Content Sync Versions Prior to 1.4.12 Drupal Events Log Track Versions either before 3.1.11, or between 4.0.0 and 4.0.1 Drupal Piwik PRO Versions Prior to 1.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-063 • https://www.drupal.org/sa-contrib-2025-062 • https://www.drupal.org/sa-contrib-2025-061 • https://www.drupal.org/sa-contrib-2025-060 • https://www.drupal.org/sa-contrib-2025-059 • https://www.drupal.org/sa-contrib-2025-058

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.