Advisory Alert

Alert Number: AAA20250529 **Date:** May 29, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Remote Code Execution Vulnerability
WatchGuard	**High**	Privilege Escalation Vulnerability
Drupal	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 VxRail Appliance - Versions 7.0.000 through 7.0.541
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000325586/dsa-2025-215-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-32433)
Description	Cisco has released a security update addressing a Remote Code Execution Vulnerability in their products. **CVE-2025-32433 -** A critical vulnerability in the Erlang/OTP SSH server was disclosed. This vulnerability could allow an unauthenticated, remote attacker to perform remote code execution (RCE) on an affected device. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Network Application, Service, and Acceleration • ConfD, ConfD Basic Prior to Versions - 7.7.19.1, 8.0.17.1, 8.1.16.2, 8.2.11.1, 8.3.8.1, 8.4.4.1 Cisco Network Management and Provisioning • Network Services Orchestrator Prior to Versions - 5.7.19.1, 6.1.16.2, 6.2.11.1, 6.3.8.1, 6.4.1.1, 6.4.4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-erlang-otp-ssh-xyZZy

Affected Product	**WatchGuard**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2025-1910)
Description	WatchGuard has released a security update addressing a Confidential Computing Vulnerability in their products. **CVE-2025-1910 -** The WatchGuard Mobile VPN with SSL Client on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Mobile VPN with SSL Client from 11.0 up to and including 12.11.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00008

Affected Product	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-48915, CVE-2025-48914, CVE-2025-48920, CVE-2025-48919, CVE-2025-48917, CVE-2025-48918, CVE-2025-48916)
Description	Drupal has released a security update addressing multiple vulnerabilities in their products. These vulnerabilities could be exploited by malicious users to cause cross site scripting and access bypass. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal COOKiES Consent Management - Versions prior to 1.2.15 Drupal Etracker - Versions prior to 3.1.0 Drupal Simple Klaro - Versions prior to 1.10.0 Drupal EU Cookie Compliance (GDPR Compliance) - Versions prior to 1.26.0 Drupal Bookable Calendar - Versions prior to 2.2.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-076 • https://www.drupal.org/sa-contrib-2025-075 • https://www.drupal.org/sa-contrib-2025-074 • https://www.drupal.org/sa-contrib-2025-073 • https://www.drupal.org/sa-contrib-2025-072 • https://www.drupal.org/sa-contrib-2025-071 • https://www.drupal.org/sa-contrib-2025-070

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-23184, CVE-2024-47535, CVE-2025-25193)
Description	IBM has released a security update addressing multiple vulnerabilities in their products **CVE-2025-23184 -** A potential denial of service vulnerability is present in versions of Apache CXF before 3.5.10, 3.6.5 and 4.0.6. In some edge cases, the CachedOutputStream instances may not be closed and, if backed by temporary files, may fill up the file system (it applies to servers and clients). **CVE-2024-47535 -** Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crashes. This vulnerability is fixed in 4.1.115. **CVE-2025-25193 -** Netty, an asynchronous, event-driven network application framework, has a vulnerability in versions up to and including 4.1.118.Final. An unsafe reading of environment file could potentially cause a denial of service in Netty. When loaded on an Windows application, Netty attempts to load a file that does not exist. If an attacker creates such a large file, the Netty application crash. A similar issue was previously reported as CVE-2024-47535. This issue was fixed, but the fix was incomplete in that null-bytes were not counted against the input limit. Commit d1fbda62d3a47835d3fb35db8bd42ecc205a5386 contains an updated fix. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM SPSS Analytic Server Versions - 3.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7234942

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.