Advisory Alert

Alert Number: AAA20251031 **Date:** October 31, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Use of Insufficiently Random Values Vulnerability
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Information Disclosure Vulnerability
cPanel	**Medium**	Out-Of-Bounds Read & Write Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in third-party components which affects Dell products. These vulnerabilities could be exploited by malicious users in order to compromise the affected systems. Dell advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	Dell Avamar Data Store Gen4T Versions 19.12, 19.10-SP1, 19.10, 19.9, 19.8 and 19.7 Dell Avamar Data Store Gen5A Versions 19.12, 19.10-SP1, 19.10, 19.9, 19.8 and 19.7 Dell Avamar Virtual Edition Versions 19.12, 19.10-SP1, 19.10, 19.9, 19.8 and 19.7 Dell Avamar Network Data Management Protocol (NDMP) Accelerator Versions 19.12, 19.10-SP1, 19.10, 19.9, 19.8 and 19.7 Dell Avamar VMware Image Backup Proxy Versions 19.12, 19.10-SP1, 19.10, 19.9, 19.8 and 19.7 Dell Networker Virtual Edition (NVE) Versions 19.5, 19.6, 19.7, 19.8, 19.9, 19.10, 19.11, 19.12 Dell PowerProtect DP Series Appliance (IDPA) Versions prior to 2.7.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000385435/

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Use of Insufficiently Random Values Vulnerability (CVE-2025-7783)
Description	IBM has released a security update addressing a critical vulnerability that exists in IBM QRadar Hub. **CVE-2025-7783**: Use of Insufficiently Random Values vulnerability in form-data allows HTTP Parameter Pollution (HPP). This vulnerability is associated with program files lib/form_data.Js. IBM advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar Hub Version 1.0.0 to 3.8.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7249661

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40300, CVE-2024-53150, CVE-2025-38352, CVE-2025-37838, CVE-2024-56767, CVE-2024-53124, CVE-2024-50299, CVE-2024-50006, CVE-2024-41006, CVE-2023-52650)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04 Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7850-1 • https://ubuntu.com/security/notices/USN-7853-1

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-58754, CVE-2023-45145, CVE-2025-27789)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-58754**: Axios is a promise based HTTP client for the browser and Node.js. When Axios prior to versions 0.30.2 and 1.12.0 runs on Node.js and is given a URL with the `data:` scheme, it does not perform HTTP. Instead, its Node http adapter decodes the entire payload into memory (`Buffer`/`Blob`) and returns a synthetic 200 response and cause the process to allocate unbounded memory and crash (DoS). **CVE-2023-45145**: Redis is an in-memory database that persists on disk. On startup, Redis begins listening on a Unix socket before adjusting its permissions to the user-provided configuration. If a permissive umask(2) is used, this creates a race condition that enables, during a short period of time, another process to establish an otherwise unauthorized connection. **CVE-2025-27789**: Babel is a compiler for writing next generation JavaScript. When using versions of Babel prior to 7.26.10 and 8.0.0-alpha.17 to compile regular expression named capturing groups, Babel will generate a polyfill for the `.replace` method that has quadratic complexity on some specific replacement pattern strings (i.e. the second argument passed to `.replace`). IBM advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	IBM QRadar Hub 1.0.0 - 3.8.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7249661

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2025-26482)
Description	Dell has released a security update addressing an information disclosure vulnerability that exists in their products. **CVE-2025-26482**: Dell PowerEdge Server BIOS and Dell iDRAC9, all versions, contains an Information Disclosure vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information Disclosure. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Precision 7920 Rack iDRAC9 Versions prior to 7.00.00.181 Precision 7920 XL Rack iDRAC9 Versions prior to 7.00.00.181 Precision 7960 Rack iDRAC9 Versions prior to 7.20.30.50 Precision 7960 XL Rack iDRAC9 Versions prior to 7.20.30.50 Precision 7920 Rack BIOS Versions prior to 2.23.0 Precision 7920 XL Rack BIOS Versions prior to 2.23.0 Precision 7960 Rack BIOS Versions prior to 2.5.4 Precision 7960 XL Rack BIOS Versions prior to 2.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000296097/dsa-2025-130

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Out-Of-Bounds Read & Write Vulnerability (CVE-2025-9230)
Description	cPanel has released a security update addressing an Out-Of-Bounds Read and Write vulnerability that exists in OpenSSL which affects EasyApache 4. **CVE-2025-9230:** An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. cPanel advises to apply this security fix at your earliest to protect your systems from potential threats.
Affected Products	All versions of OpenSSL 1.1.1w in EasyApache 4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-33-maintenance-and-security-release/

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.