TLP: WHITE

Advisory Alert

Alert Number: AAA20250605 **Date:** June 5, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Static Credential Vulnerability
ManageEngine	**Critical**	Remote Code Execution vulnerability
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
IBM	**High**	Stack-based Buffer Overflow Vulnerability
cPanel	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Apache Tomcat	**Low**	Improper Handling of Case Sensitivity vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53580, CVE-2024-39689, CVE-2024-51538, CVE-2024-53298, CVE-2025-32753)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerScale OneFS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS Versions 9.5.0.0 through 9.10.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000326339/dsa-2025-208-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Static Credential Vulnerability (CVE-2025-20286)
Description	Cisco has released security updates addressing a Static Credential Vulnerability that exists in third party products which affect Cisco Identity Services Engine. **CVE-2025-20286** - A vulnerability in Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI) cloud deployments of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to access sensitive data, execute limited administrative operations, modify system configurations, or disrupt services within the impacted systems. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco ISE Release 3.1, 3.2, 3.3 and 3.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7

Affected Product	**ManageEngine**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution vulnerability (CVE-2025-3835)
Description	ManageEngine has released security updates addressing a Remote Code Execution vulnerability that exists in Exchange Reporter Plus. **CVE-2025-3835** - A vulnerability in Content Search module allows attackers to execute custom arbitrary commands on target servers. This vulnerability could, in rare scenarios, impact system integrity. ManageEngine advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Exchange Reporter Plus Build 5721 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.manageengine.com/products/exchange-reports/advisory/CVE-2025-3835.html

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (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)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third party products which affects Dell Networking Products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VEP1400 (VEP1425/1445/1485) Firmware Versions prior to 2.6 Dell SD-WAN EDGE620/640/680 Firmware Versions prior to 2.6 Dell SD-WAN EDGE610/610-LTE Firmware Versions prior to 2.6 PowerSwitch Z9432F-ON Firmware Versions prior to 3.51.5.1-21 PowerSwitch S5448F-ON Firmware Versions prior to 3.52.5.1-12 PowerSwitch N2200-ON Series Firmware Versions prior to 3.45.5.1-31 PowerSwitch N3200-ON Series Firmware Versions prior to 3.45.5.1-31 PowerSwitch E3200-ON Series Firmware Versions prior to 3.57.5.1-5 PowerSwitch Z9264F-ON Firmware Versions prior to 3.42.5.1-21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000328454/dsa-2025-216-security-update-for-dell-networking-products-for-multiple-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37097, CVE-2025-37098, CVE-2025-37099)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Code Execution, Directory Traversal and Disclosure of Information. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Insight Remote Support versions prior to 7.15.0.646
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04878en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Stack-based Buffer Overflow Vulnerability (CVE-2024-7254)
Description	IBM has released security updates addressing a Stack-based Buffer Overflow Vulnerability that exists in IBM Db2 Server. **CVE-2024-7254** - Any project that parses untrusted Protocol Buffers data containing an arbitrary number of nested groups / series of SGROUP tags can corrupted by exceeding the stack limit i.e. StackOverflow. Parsing nested groups as unknown fields with DiscardUnknownFieldsParser or Java Protobuf Lite parser, or against Protobuf map fields, creates unbounded recursions that can be abused by an attacker. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7235067

Affected Product	**cPanel**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-47947, CVE-2025-48866, CVE-2025-5025, CVE-2025-4947)
Description	cPanel has released security updates for EasyApache 4 addressing multiple vulnerabilities in third party products. These vulnerabilities could be exploited by malicious users to compromise the affected system. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 with all versions of ModSecurity 2 through 2.9.9 EasyApache 4 with all versions of libcurl through 8.13.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-18-maintenance-and-security-release/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-57850, CVE-2024-56596, CVE-2024-56551, CVE-2024-53168, CVE-2024-53155, CVE-2024-47701, CVE-2024-42301, CVE-2024-26966, CVE-2023-52458, CVE-2021-47353, CVE-2021-47211)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 16.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7554-1 • https://ubuntu.com/security/notices/USN-7553-1

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20261, CVE-2025-20163, CVE-2025-20278, CVE-2025-20276, CVE-2025-20277, CVE-2025-20279, CVE-2025-20275, CVE-2025-20259, CVE-2025-20130, CVE-2025-20273, CVE-2025-20129)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Command Injection, Cross-site Scripting, Remote Code Execution, Information Disclosure. 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-ucs-ssh-priv-esc-2mZDtdjM • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-shkv-snQJtjrp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vos-command-inject-65s2UCYy • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-multi-UhOTvPGL • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-uccx-editor-rce-ezyYZte8 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-te-endagent-filewrt-zNcDqNRJ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-file-upload-P4M8vwXY • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-icm-xss-cfcqhXAg • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ccp-info-disc-ZyGerQpd

Affected Product	**Apache Tomcat**
Severity	**Low**
Affected Vulnerability	Improper Handling of Case Sensitivity vulnerability (CVE-2025-46701)
Description	Apache has released security updates addressing an Improper Handling of Case Sensitivity vulnerability that exists Tomcat's GCI servlet. **CVE-2025-46701** - Improper Handling of Case Sensitivity vulnerability in Apache Tomcat's GCI servlet allows security constraint bypass of security constraints that apply to the pathInfo component of a URI mapped to the CGI servlet. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat 11.0.0-M1 to 11.0.6 Apache Tomcat 10.1.0-M1 to 10.1.40 Apache Tomcat 9.0.0.M1 to 9.0.104
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-11.html • https://tomcat.apache.org/security-10.html • https://tomcat.apache.org/security-9.html

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.