Advisory Alert

Alert Number: **AAA20250815** **Date:** **August 15, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Remote Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
HPE	**High, Medium, Low**	Multiple Vulnerabilities
PostgreSQL	**High, Low**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities
Palo Alto Networks	**Low**	Cleartext Storage of Sensitive Information Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-20265)
Description	Cisco has released security updates addressing a Remote Code Execution Vulnerability that exists in Cisco Firewall Management Center Software. **CVE-2025-20265** - This vulnerability is due to a lack of proper handling of user input during the authentication phase. An attacker could exploit this vulnerability by sending crafted input when entering credentials that will be authenticated at the configured RADIUS server. A successful exploit could allow the attacker to execute commands at a high privilege level. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure Firewall Management Center Software releases 7.0.7 and 7.7.0 if they have RADIUS authentication enabled
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell VxRail Appliance. 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	Dell VxRail Appliance versions 8.0.000 through 8.0.330
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000335212/dsa-2025-244-security-update-for-dell-vxrail-for-multiple-third-party-component-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-47252, CVE-2024-8176, CVE-2025-23048, CVE-2025-32414, CVE-2025-32415, CVE-2025-47947, CVE-2025-49630, CVE-2025-49812)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in JBoss Core Services. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat JBoss Core Services Text-Only Advisories x86_64 Red Hat JBoss Core Services 1 for RHEL 8 x86_64 Red Hat JBoss Core Services 1 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:13681 • https://access.redhat.com/errata/RHSA-2025:13680

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20217, CVE-2025-20222, CVE-2025-20148, CVE-2025-20244, CVE-2025-20133, CVE-2025-20243, CVE-2025-20134, CVE-2025-20136, CVE-2025-20251, CVE-2025-20224, CVE-2025-20225, CVE-2025-20263, CVE-2025-20127, CVE-2025-20268, CVE-2025-20235, CVE-2025-20218, CVE-2025-20220, CVE-2025-20306, CVE-2025-20301, CVE-2025-20302, CVE-2025-20135, CVE-2025-20237, CVE-2025-20238, CVE-2025-20219, CVE-2025-20239)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Access Bypass, Cross-Site Scripting, Command Injection. 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/publicationListing.x?product=Cisco&sort=-day_sir#~Vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-54090, CVE-2025-48976)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM WebSphere products. **CVE-2025-54090** - A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true". Users are recommended to upgrade to version 2.4.65, which fixes the issue. IBM HTTP Server used by IBM WebSphere Application Server is affected by a security bypass vulnerability due to the included Apache HTTP Server. This affects IBM HTTP Server with IFPH67153 installed. **CVE-2025-48976** - Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. This vulnerability in Apache Commons FileUpload which affects IBM WebSphere Application Server traditional and affects IBM WebSphere Application Server Liberty IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server versions 9.1 and 9.0 IBM WebSphere Application Server versions 9.0 and 8.5 IBM WebSphere Application Server Liberty versions 17.0.0.3 - 25.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7242165 • https://www.ibm.com/support/pages/node/7242088

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20613, CVE-2025-21096, CVE-2025-22853, CVE-2025-20053, CVE-2025-24305, CVE-2025-21090)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Information Disclosure, and Privilege Escalation. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Alletra 4110 - Prior to 2.60_08-07-2025 HPE Alletra 4120 - Prior to 2.60_08-07-2025 HPE Alletra 4140 - Prior to 2.60_08-07-2025 HPE ProLiant DL110 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant DL320 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL360 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL380 Gen11 Server - Prior to 2.60_08-07-2025 HPE ProLiant DL380a Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant DL560 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant ML110 Gen11 - Prior to 2.60_08-07-2025 HPE ProLiant ML350 Gen11 Server - Prior to 2.60_08-07-2025 HPE Compute Edge Server e930t - Prior to 2.60_08-07-2025 HPE Synergy 480 Gen11 Compute Module - Prior to 2.60_08-07-2025 HPE StoreEasy 1470 Performance - Prior to 2.60_08-07-2025 (U63 ROM Family) HPE StoreEasy 1470 Storage - Prior to 2.60_08-07-2025 (U63 ROM Family) HPE StoreEasy 1570 Performance - Prior to 2.60_08-07-2025 (U63 ROM Family) HPE StoreEasy 1570 Storage - Prior to 2.60_08-07-2025 (U63 ROM Family) HPE StoreEasy 1670 Performance Storage - Prior to 2.60_08-07-2025 (U54 ROM Family) HPE StoreEasy 1670 Storage - Prior to 2.60_08-07-2025 (U54 ROM Family) HPE StoreEasy 1870 Performance Storage - Prior to 2.60_08-07-2025 (U54 ROM Family) HPE StoreEasy 1870 Storage - Prior to 2.60_08-07-2025 (U54 ROM Family)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04916en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04917en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04926en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04927en_us&docLocale=en_US

Affected Product	**PostgreSQL**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-8713, CVE-2025-8714, CVE-2025-8715)
Description	Postgres has released security updates addressing multiple vulnerabilities that exist in PostgreSQL. **CVE-2025-8713** - PostgreSQL optimizer statistics allow a user to read sampled data within a view that the user cannot access. Separately, statistics allow a user to read sampled data that a row security policy intended to hide. PostgreSQL maintains statistics for tables by sampling data available in columns; this data is consulted during the query planning process. **CVE-2025-8714** - Untrusted data inclusion in pg_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands. pg_dumpall is also affected. pg_restore is affected when used to generate a plain-format dump. **CVE-2025-8715** - Improper neutralization of newlines in pg_dump in PostgreSQL allows a user of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands inside a purpose-crafted object name. The same attacks can achieve SQL injection as a superuser of the restore target server. pg_dumpall, pg_restore, and pg_upgrade are also affected. Postgres advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PostgreSQL Versions before 17.6, 16.10, 15.14, 14.19, and 13.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.postgresql.org/about/news/postgresql-176-1610-1514-1419-1322-and-18-beta-3-released-3118/

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38738, CVE-2025-36612, CVE-2025-36613)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell SupportAssist software and installer. **CVE-2025-38738** - SupportAssist for Home PCs Installer exe version(s) 4.8.2.29006 and prior, contain(s) an Incorrect Privilege Assignment vulnerability in the Installer. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges. **CVE-2025-36612** - SupportAssist for Business PCs, version(s) 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges. **CVE-2025-36613** - SupportAssist for Home PCs versions 4.6.3 and prior and SupportAssist for Business PCs versions 4.5.3 and prior, contain(s) an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to unauthorized access. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SupportAssist for Business PCs versions prior to 4.5.3 SupportAssist for Home PCs versions prior to 4.8.2.29006
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000356690/dsa-2025-296-security-update-for-dell-supportassist-for-home-pcs-and-dell-supportassist-for-business-pcs-vulnerabilities

Affected Product	**Palo Alto Networks**
Severity	**Low**
Affected Vulnerability	Cleartext Storage of Sensitive Information Vulnerability (CVE-2025-2182)
Description	Palo Alto Networks has released security updates addressing a Cleartext Storage of Sensitive Information Vulnerability that exists in PAN-OS running on PA-7500 Series devices. **CVE-2025-2182** - A problem with the implementation of the MACsec protocol in Palo Alto Networks PAN-OS results in the cleartext exposure of the connectivity association key (CAK). This issue is only applicable to PA-7500 Series devices which are in an NGFW cluster. A user who possesses this key can read messages being sent between devices in a NGFW Cluster. Palo Alto Networks advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Following PAN-OS versions running on PA-7500 Series devices which are in an NGFW cluster (A MACsec policy must be configured and enabled for the NGFW cluster): • PAN-OS 11.2 – versions prior to 11.2.8 • PAN-OS 11.1 – versions prior to 11.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2025-2182

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.