Advisory Alert

Alert Number: AAA20250904 **Date:** September 4, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**High**	Local Escalation of Privilege Vulnerability
NetApp	**High**	Security Update
Dell	**High**	Multiple Vulnerabilities
IBM	**High**	Denial of Service Vulnerability
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their product. 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	RecoverPoint for Virtual Machines - Versions prior to 6.0.SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000358406/dsa-2025-308-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-third-party-component-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Local Escalation of Privilege Vulnerability (CVE-2025-32463)
Description	HPE has released a security update addressing a Local escalation of privilege vulnerability that exists in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE SN2010M 25GbE 18SFP28 4QSFP28 Power to Connector Airflow Half Width Switch with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN2100M 100GbE 16QSFP28 Power to Connector Airflow Half Width Switch SN2100M with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN3420M 25GbE 48SFP28 12QSFP28 Power to Connector Airflow Switch SN3420M with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN3700cM 100GbE 32QSFP28 Power to Connector Airflow Switch SN3700cM with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN3700M 200GbE 32QSFP56 Power to Connector Airflow Switch SN3700M with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN4600cM 100GbE 64QSFP28 Power to Connector Airflow Switch SN4600cM with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1 • HPE SN4700M 400GbE 32QSFPDD Power to Connector Airflow Switch SN4700M with NVIDIA Cumulus - NVIDIA Cumulus 5.9.2, and 5.11.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst04945en_us&docLocale=en_US

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2025-27363)
Description	NetApp has released a security update addressing a vulnerability that exists in Active IQ Unified Manager. **CVE-2025-27363** - Multiple NetApp products incorporate Freetype. Freetype versions through 2.13.0 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Active IQ Unified Manager for VMware vSphere
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20250613-0008

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their 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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000364913/dsa-2025-297-security-update-for-dell-poweredge-server-for-intel-2025-security-advisories-2025-3-ipu • https://www.dell.com/support/kbdoc/en-us/000364903/dsa-2025-337-security-update-for-dell-enterprise-sonic-distribution-vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2025-48976)
Description	IBM has released a security update addressing a denial-of-service vulnerability that exists in their product. **CVE-2025-48976** - Allocation of resources for multipart headers with insufficient limits enabled a DoS vulnerability in Apache Commons FileUpload. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Hybrid Edition - 5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7243922

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20328, CVE-2025-20335, CVE-2025-20336, CVE-2025-20330, CVE-2025-20280, CVE-2025-20270, CVE-2025-20287, CVE-2025-20326)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause cross-site scripting (XSS), information disclosure, and cross-site request forgery (CSRF) attacks. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Cisco Webex Meetings • Desk Phone 9800 Series • IP Phone 7800 and 8800 Series - Earlier than 14.3 • IP Phone 8821 - Earlier than 11 • Video Phone 8875 - 2.3(1)SR1 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-xss-55bv8hhm#vp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-phone-write-g3kcC5Df • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-imp-xss-XQgu4HSG • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-stored-xss-XjQZsyCP • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-info-dis-zhPPMfgz • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epni-arb-file-upload-jjdM2P83 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-csrf-w762pRYd

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.