Advisory Alert

Alert Number: AAA20260917 **Date:** September 17, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Hitachi	**High**	Remote Code Execution Vulnerability
Dell	**High**	Uncontrolled Search Path Element Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
cPanel	**Medium**	Buffer Overflow Vulnerability

Description

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-42374, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2022-28391, CVE-2022-48174, CVE-2025-46394, CVE-2025-60876, CVE-2024-25943, CVE-2025-22396, CVE-2026-26945, CVE-2026-26948, CVE-2024-38796, CVE-2024-52533, CVE-2024-2961, CVE-2025-31648, CVE-2025-22885, CVE-2025-27572, CVE-2025-27940, CVE-2025-30513, CVE-2025-31944, CVE-2025-32007, CVE-2025-32467, CVE-2023-52340, CVE-2023-6780, CVE-2024-45490, CVE-2024-45491, CVE-2024-45492, CVE-2024-50602, CVE-2024-42154, CVE-2026-6923, CVE-2023-48795, CVE-2024-6387, CVE-2025-26466, CVE-2025-11187, CVE-2025-15467, CVE-2025-15468, CVE-2025-15469, CVE-2025-66199, CVE-2025-68160, CVE-2025-69418, CVE-2025-69419, CVE-2025-69420, CVE-2025-69421, CVE-2026-22795, CVE-2026-22796, CVE-2026-23855, CVE-2025-29088)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Object Storage (Firmware Catalog < 2.6.3): * ECS: Prior to 3.8.1.7 * ObjectScale: Prior to 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000509706/dsa-2026-401-security-update-for-dell-ecs-and-objectscale-multiple-third-party-component-vulnerabilities

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76460, CVE-2026-20242, CVE-2026-20329, CVE-2026-20330, CVE-2026-20331, CVE-2026-20332, CVE-2026-20333, CVE-2026-20334, CVE-2026-20335, CVE-2026-20336, CVE-2026-20130, CVE-2026-20192, CVE-2026-20194, CVE-2026-20234, CVE-2026-20237, CVE-2026-20287, CVE-2026-20322, CVE-2026-20325, CVE-2026-20326, CVE-2026-20360, CVE-2026-20361, CVE-2026-76409, CVE-2026-20305, CVE-2026-20306, CVE-2026-20282, CVE-2026-20283, CVE-2026-20284, CVE-2026-76423, CVE-2026-76424, CVE-2026-76425, CVE-2026-76426, CVE-2026-76427, CVE-2026-76428, CVE-2026-20176, CVE-2026-20211, CVE-2026-20307, CVE-2026-20079)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco Nexus Dashboard Cisco Identity Services Engine (ISE) & Passive Identity Connector (ISE-PIC) Cisco Secure FMC Software Cisco Secure Firewall Management Center (FMC) Software Cisco Secure Firewall Adaptive Security Appliance (ASA) Software Cisco Secure Firewall Threat Defense (FTD) Software Cisco Security Cloud Control (SCC)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-javarce-y2NypXwk • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-asaftdfmc-uvpPROhN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ndw1-psFvnrg • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-e2CuZCYZ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-vul-ymSsTLCc • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2

Vendor	**Hitachi**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-1978)
Description	Hitachi has released a security update addressing a vulnerability that exists in their products. **CVE-2025-1978:** A vulnerability exists in the management software (Storage Navigator) of Hitachi Disk Array Systems that involves remote code execution vulnerability. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, F350, F370, F700, F900 Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H Hitachi Virtual Storage Platform One Block 23, One Block 24, One Block 26, One Block 28
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_307.html

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Uncontrolled Search Path Element Vulnerability (CVE-2026-56795)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-56795:** Dell Server Update Utility, versions prior to 26.07.01, contains an Uncontrolled Search Path Element vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Driver Pack For Windows OS - Versions prior to 26.07.01 Dell Driver Pack For Linux OS - Versions prior to 26.07.01 Dell Server Update Utility, Windows 64-bit format - Versions prior to 26.07.01 Dell Server Update Utility, Linux 64-bit format - Versions prior to 26.07.01
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000509930/dsa-2026-422-security-update-for-dell-server-update-utility-suu-vulnerability

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43114, CVE-2026-45998, CVE-2026-46054, CVE-2026-46056, CVE-2026-53016, CVE-2026-53006, CVE-2026-53071, CVE-2026-53196, CVE-2026-63886, CVE-2026-64304, CVE-2026-46150, CVE-2026-52933, CVE-2026-53000, CVE-2026-63888, CVE-2026-63887, CVE-2026-64268, CVE-2026-64438, CVE-2025-40026)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x Red Hat OpenShift Container Platform 4.19 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.19 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.19 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.19 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.19 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.19 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.19 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.19 for RHEL 8 aarch64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.6 x86_64 * Red Hat Enterprise Linux Server - AUS 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:67723 • https://access.redhat.com/errata/RHSA-2026:66370 • https://access.redhat.com/errata/RHSA-2026:68100 • https://access.redhat.com/errata/RHSA-2026:68131

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76438, CVE-2026-20285, CVE-2026-20286, CVE-2026-20235, CVE-2026-76431, CVE-2026-76432, CVE-2026-76433, CVE-2026-76434, CVE-2026-20071, CVE-2026-20072, CVE-2026-76439, CVE-2026-76444, CVE-2026-76446, CVE-2026-76447, CVE-2026-76448, CVE-2026-76449, CVE-2026-76450, CVE-2026-76451, CVE-2026-20309, CVE-2026-20350, CVE-2026-20154, CVE-2026-20250, CVE-2026-20135, CVE-2026-20352, CVE-2026-20247, CVE-2026-20300, CVE-2026-20349, CVE-2026-20316)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Cisco BroadWorks CommPilot Application Software Cisco ISE Passive Identity Connector (ISE-PIC) Cisco Identity Services Engine (ISE) Cisco ThousandEyes Virtual Appliance Cisco Secure Firewall 3100 Series and 4200 Series Cisco Secure Firewall ASA Software Cisco Secure FTD Software & Secure FMC Software & Cisco Secure Firewall Management Center (FMC)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10723, CVE-2026-10822, CVE-2026-11622, CVE-2026-11721, CVE-2026-13204, CVE-2026-13321, CVE-2026-11331, CVE-2026-12617)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AIX - Versions 7.2 & 7.3 VIOS - Version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7287477

Vendor	**cPanel**
Severity	**Medium**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-90439)
Description	cPanel has released a security update addressing a vulnerability that exists in their products. **CVE-2026-90439:** When using HTTP/3 with OpenSSL versions <= OpenSSL 3.5.0 under certain configurations, a limited heap buffer overflow could happen while processing a TLS handshake. This can happen in a non-deterministic manner that is beyond the attacker's control. This may cause a heap buffer overflow in the NGINX worker process leading to a restart and/or limited data corruption. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or limited data corruption. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 • ea-nginx v1.31.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.