Advisory Alert

Alert Number: AAA20260116 **Date:** January 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Remote Code Execution Vulnerability
HPE	**Critical**	Remote Code Execution Vulnerability
Cisco	**Critical**	Remote Code Execution Vulnerability
Drupal	**Critical**	Access Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**	Unauthenticated Memory Disclosure Vulnerability
Palo Alto	**High**	Denial of Service Vulnerability
Juniper	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-46981)
Description	Juniper has released security updates addressing a vulnerability that exists in their Junos Space Products. **CVE-2024-46981-** a vulnerability in Redis (the open-source in-memory database) where an authenticated user can execute specially crafted Lua scripts that manipulate the garbage collector and potentially lead to remote code execution (RCE). The flaw arises from improper memory management related to use-after-free conditions when executing untrusted Lua code. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos Space - All versions prior to 24.1R5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2026-01-Security-Bulletin-Junos-Space-Multiple-vulnerabilities-resolved-in-24-1R5-release

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-37164)
Description	HPE has released security updates addressing a vulnerability that exists in their HPE OneView Product software. **CVE-2025-37164 -** a critical unauthenticated remote code execution (RCE) vulnerability in HPE OneView caused by improper input handling in a network-accessible API. A remote attacker can exploit this flaw without authentication to execute arbitrary code with OneView application privileges. Successful exploitation may lead to full system compromise, impacting confidentiality, integrity, and availability of the managed infrastructure. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE OneView - All versions through v10.20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04985en_us&docLocale=en_US

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-20393)
Description	Cisco has released security updates addressing a vulnerability that exists in their AsyncOS based Products. **CVE-2025-20393 -** remote code execution (RCE) vulnerability in Cisco AsyncOS Software used by Cisco Secure Email Gateway (SEG) and Cisco Secure Email and Web Manager (SEWM). It arises from improper input validation (CWE-20) and allows unauthenticated remote attackers to execute arbitrary commands with root privileges on affected appliances. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure Email Gateway • AsyncOS versions 14.2 and earlier • AsyncOS version 15.0 / 15.5 / 16.0 Cisco Secure Email and Web Manager • AsyncOS versions 15.0 and earlier • AsyncOS versions 15.5 / 16.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2026-0948)
Description	Drupal has released security updates addressing a vulnerability that exists in the Microsoft Entra ID SSO Login contributed module. **CVE-2026-0948 -** a critical access bypass vulnerability in the Microsoft Entra ID SSO Login module for Drupal, caused by insufficient validation of API responses from Microsoft Entra ID. A remote attacker can exploit this flaw to perform complete account takeover of any user, including site administrators, without requiring credentials or email access. Successful exploitation may compromise site access and administrative control, severely impacting the confidentiality and integrity of a Drupal site. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Microsoft Entra ID SSO Login module for Drupal - All versions prior to v1.0.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-005

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-53322, CVE-2023-53675, CVE-2025-38051, CVE-2025-39971, CVE-2025-68285)
Description	Red Hat 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 and privilege escalation. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux Server - AUS 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:0643

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-22278, CVE-2026-22280, CVE-2026-22279, CVE-2026-22281)
Description	Dell 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 and privilege escalation. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS Versions prior to 9.13.0.0 PowerScale OneFS Versions 9.5.0.0 through 9.5.1.5 PowerScale OneFS Versions 9.6.0.0 through 9.7.1.10 PowerScale OneFS Versions 9.8.0.0 through 9.10.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000415586/dsa-2026-049-security-update-for-dell-powerscale-onefs-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Unauthenticated Memory Disclosure Vulnerability (CVE-2025-14847)
Description	IBM has released security updates addressing a vulnerability that exists in their IBM WebSphere products. **CVE-2025-14847 -** a high-severity unauthenticated memory disclosure vulnerability in MongoDB's zlib compression handling that allows remote attackers to leak uninitialized heap memory. By sending specially crafted compressed network packets, an attacker can cause the server to return fragments of internal memory before authentication, potentially exposing sensitive data such as credentials and tokens. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Automation (v1.10.0 and v1.11.0)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7257005

Affected Product	**Palo Alto**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-0227)
Description	Palo Alto has released security updates addressing a vulnerability that exists in their products. **CVE-2026-0227 -** a denial-of-service (DoS) vulnerability in Palo Alto Networks PAN-OS affecting GlobalProtect Gateway and Portal configurations, where an unauthenticated attacker can send crafted network traffic to disrupt firewall operation. Repeated exploitation can force the firewall into maintenance mode, significantly impacting availability and remote access services such as GlobalProtect. Palo Alto advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PAN-OS 12.1 prior to 12.1.3-h3 / 12.1.4 PAN-OS 11.2 prior to 11.2.4-h15 / 11.2.7-h8 / 11.2.10-h2 PAN-OS 11.1 prior to 11.1.4-h27 / 11.1.6-h23 / 11.1.10-h9 / 11.1.13 PAN-OS 10.2 prior to 10.2.7-h32 / 10.2.10-h30 / 10.2.13-h18 / 10.2.16-h6 / 10.2.18-h1 PAN-OS 10.1 prior to 10.1.14-h20
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0227

Affected Product	**Juniper**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Juniper has released monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users in order to compromise systems and data. Juniper 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://supportportal.juniper.net/s/global-search/%40uri#sortCriteria=date%20descending&f-sf_primarysourcename=Knowledge&f-sf_articletype=Security%20Advisories&numberOfResults=50

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20076, CVE-2026-20047, CVE-2026-20075)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-20076 -** An authenticated stored cross-site scripting (XSS) issue in the web UI of Cisco Identity Services Engine (ISE) allows an authenticated remote attacker to inject malicious script code that executes in a victim's browser session. **CVE-2026-20047 -** An authenticated XSS flaw in the web-based interface of Cisco ISE and Cisco ISE Passive Identity Connector (ISE-PIC) due to improper input validation, letting an attacker execute arbitrary script in the context of a user's browser session. **CVE-2026-20075 -** A stored cross-site scripting (XSS) vulnerability in the web UIs of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure, caused by insufficient input validation. An authenticated admin can inject harmful scripts affecting other users' sessions. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Identity Services Engine (ISE) • v3.1 and earlier • v3.2, v3.3, v3.4 and v3.5 Cisco ISE Passive Identity Connector (ISE-PIC) • v3.2 and earlier • v3.3, v3.4 and v3.5 Cisco Evolved Programmable Network Manager (EPNM) • v7.0 and earlier • v7.1, v8.0, and v8.1 Cisco Prime Infrastructure • v3.9 and earlier • v3.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-9TDh2kx • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-964cdxW5 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-pi-stored-xss-GEkX8yWK

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.