Advisory Alert

Alert Number: AAA20261105 **Date:** November 5, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
WatchGuard	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Buffer Overflow Vulnerability
Drupal	**High**	Multiple Vulnerabilities
cPanel	**High**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
WatchGuard	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Hitachi	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71066, CVE-2026-46259, CVE-2026-64534, CVE-2026-68159, CVE-2026-68156, CVE-2026-68155, CVE-2026-68476, CVE-2026-74669, CVE-2026-74641, CVE-2026-80714, CVE-2026-89481, CVE-2026-98432)
Description	Red Hat 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. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• 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-2026:94996

Vendor	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-121639, CVE-2026-121638, CVE-2026-121640)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-121639:** A Missing Authentication for Critical Function vulnerability in WatchGuard AuthPoint Gateway allows a remote unauthenticated attacker with network access to the AuthPoint Gateway host to disrupt authentication services and delete the local directory synchronization configuration. **CVE-2026-121638:** An Improper Certificate Validation vulnerability in WatchGuard AuthPoint Gateway allows an attacker with an on-path network position to intercept and modify communications between the AuthPoint Gateway and local authentication providers. **CVE-2026-121640:** An Authentication Bypass by Capture-replay vulnerability in WatchGuard AuthPoint Gateway allows an attacker who has observed a legitimate request between AuthPoint Gateway components to replay it and perform unauthorized administrative actions, including disrupting authentication services. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AuthPoint Authentication Gateway Versions: >= 1.0, < 7.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.watchguard.com/CVE-2026-121640/ • https://psirt.watchguard.com/CVE-2026-121638/ • https://psirt.watchguard.com/CVE-2026-121639/

Vendor	**Dell**
Severity	**Critical**
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 systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• NetWorker - Versions prior to 19.14.0.1 • Dell Avamar Data Store Gen4T - Versions 19.10, 19.10-SP1, 19.12 • Dell Avamar Data Store Gen5A - Versions 19.10, 19.10-SP1, 19.12 • Dell Avamar Virtual Edition - Versions 19.10, 19.10-SP1, 19.12 • Dell Avamar Network Data Management Protocol (NDMP) Accelerator - Versions 19.10, 19.10-SP1, 19.12 • Dell Avamar VMware Image Backup Proxy - Versions 19.10, 19.10-SP1, 19.12 • Dell Networker Virtual Edition (NVE) - Versions 19.5, 19.6, 19.7, 19.8, 19.9, 19.10, 19.11, 19.12,19.13,19.14 • Dell PowerProtect DP Series Appliance (IDPA - Versions prior to 2.7.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000529612/dsa-2026-483-security-update-for-dell-avamar-dell-networker-virtual-edition-nve-and-dell-powerprotect-dp-series-appliance-dell-integrated-data-protection-appliance-idpa-multiple-third-party-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000529819/dsa-2026-238-security-update-for-dell-networker-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000529808/dsa-2026-253-security-update-for-dell-networker-multiple-vulnerabilities

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2026-111497)
Description	IBM has released a security update addressing a vulnerability that exists in their products. **CVE-2026-111497:** A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• QRadar - Versions 7.5.0 - 7.5.0 UP16 IF02 • QRadar - Versions 7.6.0.0 - 7.6.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7295464

Vendor	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-118565, CVE-2026-122066)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-118565:** Integration with GroupEx PRO system, decoupled from Open Y. The module does not sufficiently validate user inputs in some scenarios, potentially leading to arbitrary remote code execution. **CVE-2026-122066:** This module enables you to send messages ("Notifications") to users upon a certain Workflow state change. The module doesn't sufficiently protect the Notification settings page where an attacker can make unauthorized changes. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Module: • GroupEx PRO (Daxko) integration- Versions prior to 2.2.1 • Workflow Notifications - Versions prior to 3.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2026-278 • https://www.drupal.org/sa-contrib-2026-297

Vendor	**cPanel**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-14181, CVE-2026-91765)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2025-14181:** The SOAP HTTP client guards its response buffer growth with a check that relies on signed integer overflow, which is undefined behaviour and is not guaranteed to trigger. When the check is optimised away, a malicious SOAP server can make the client allocate a buffer far smaller than the data it then writes into it, producing a heap buffer overflow. **CVE-2026-91765:** cleanup_xml_node() in the SOAP XML parser recurses once per XML nesting level with no depth limit. An unauthenticated attacker can post a SOAP request containing tens of thousands of nested elements to any SoapServer endpoint, exhaust the stack and crash the process. The same unbounded recursion exists in the SOAP value decoder and in the WSDL node search helper. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache: • ea-php74 & ea-php74-meta • ea-php80 & ea-php80-meta • ea-php81 & ea-php81-meta • ea-podman • ea-ruby27-rubygem-rack
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84445, CVE-2026-44432, CVE-2026-11332, CVE-2026-44431, CVE-2026-33814, CVE-2026-107176, CVE-2026-39825, CVE-2026-46597, CVE-2026-52929, CVE-2026-64541, CVE-2026-74586, CVE-2026-80864, CVE-2026-80863, CVE-2026-89488, CVE-2026-93579, CVE-2026-93569, CVE-2026-93568, CVE-2026-93567, CVE-2026-93492, CVE-2026-59903, CVE-2026-84501, CVE-2026-59969, CVE-2026-89058, CVE-2026-89059, CVE-2026-90852, CVE-2026-90560, CVE-2026-68497, CVE-2026-89046, CVE-2026-87824, CVE-2026-87795, CVE-2026-87877, CVE-2026-87825, CVE-2026-59296, CVE-2026-66257, CVE-2026-66273, CVE-2026-17615, CVE-2026-66274, CVE-2026-64378, CVE-2026-72222, CVE-2026-72221, CVE-2026-72080, CVE-2026-90315, CVE-2026-98974, CVE-2026-68162, CVE-2026-68452, CVE-2026-68451, CVE-2026-74588, CVE-2026-74752, CVE-2026-80553, CVE-2026-80571, CVE-2026-80584, CVE-2026-89479, CVE-2026-98403)
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	RHEL 10 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, s390x, x86_64 • Hidden Content: x86_64 RHEL 10.2: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • 4 Years of Updates/Support: aarch64, ppc64le, s390x, x86_64 • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 9 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, s390x, x86_64 RHEL 9.8: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 8 Base: • Base OS: aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder: aarch64, ppc64le, x86_64 RHEL 8.10: • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 Other products: • Red Hat OpenShift Container Platform • JBoss Enterprise Application Platform Text-Only Advisories: x86_64 • JBoss Enterprise Application Platform 7.4 ELS 7: x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:95054 • https://access.redhat.com/errata/RHSA-2026:92281 • https://access.redhat.com/errata/RHSA-2026:92280 • https://access.redhat.com/errata/RHSA-2026:95212 • https://access.redhat.com/errata/RHSA-2026:95221 • https://access.redhat.com/errata/RHSA-2026:95367 • https://access.redhat.com/errata/RHSA-2026:95370

Vendor	**WatchGuard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-121637)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. **CVE-2026-121637:** An improper integrity validation vulnerability in WatchGuard AuthPoint Gateway's LDAP authentication callback allows a network attacker who has obtained a valid header signature to forge the authentication result and transaction identifier in the request body, resulting in unauthorized session outcomes. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AuthPoint Authentication Gateway Versions: >= 1.0, < 7.6.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-121637/

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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	Connectrix Switches and Directors Versions: • Versions prior to 3.0.1 • Versions prior to 3.0.0a • Versions prior to 2.4.0b
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000529579/dsa-2026-476-security-update-for-dell-connectrix-b-series-sannav-vulnerabilities

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76419, CVE-2026-76506, CVE-2026-20241)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-76419:** This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. **CVE-2026-76506:** This vulnerability is due to insufficient validation of user-supplied input in an HTTP request. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected endpoint on an affected device. A successful exploit could allow the attacker to execute arbitrary commands, write arbitrary files to the filesystem, and obtain sensitive information. To exploit this vulnerability, the attacker must have valid user credentials on the affected device. **CVE-2026-20241:** This vulnerability is due to improper authorization checks. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to bypass authorization to obtain an endpoint certificate. Cisco advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Cisco Unified CM • Cisco Unified CM SME • Cisco UCS Central Software • Cisco ISE • Cisco ISE-PIC
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-xss-5mQn2U5z • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucs-rce-LzHSFRDQ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cert-mE9BD5GO

Vendor	**Hitachi**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Hitachi 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. Hitachi advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Hitachi Virtual Storage Platform E590, E790, E990, E1090, E590H, E790H, E1090H • Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900 • Hitachi Virtual Storage Platform F350, F370, F700, F900 • Hitachi Virtual Storage Platform G100, G200, G400, G600, G800 • Hitachi Virtual Storage Platform F400, F600, F800 • Hitachi Virtual Storage Platform N400, N600, N800
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/09.html

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-122075, CVE-2026-118566)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-122075:** The module doesn't sufficiently check if a user has permission to change publication or unpublication dates. This might cause certain information to be publicly disclosed ahead of the scheduled time, or content to become inaccessible earlier or later than planned. **CVE-2026-118566:** The Content Synchronizer module allows content to be exported and imported between Drupal sites via uploaded archive files. The module doesn't sufficiently sanitize input passed to its client-side code, leading to a DOM-based cross-site scripting (XSS) vulnerability. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Module: • Scheduler - Versions: <1.7.0 || >=2.2.0 <2.2.3 || 2.0.* || 2.1.* || >= 2.3.0 <2.3.1 • Content Synchronizer - Versions prior to 4.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2026-306 • https://www.drupal.org/sa-contrib-2026-294

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.