



Advisory Alert

Alert Number: AAA20261002 Date: October 2, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Fortinet	Critical	Path Traversal Vulnerability
WatchGuard	Critical	Missing Authentication Vulnerability
Dell	Critical	Multiple Vulnerabilities
IBM	Critical	Multiple Vulnerabilities
Red Hat	High, Medium	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
Apache HTTP Server	Medium, Low	Multiple Vulnerabilities
F5	Low	Multiple Vulnerabilities

Description

Vendor	Fortinet
Severity	Critical
Affected Vulnerability	Path Traversal Vulnerability (CVE-2026-104286)
Description	Fortinet has released a security update addressing a vulnerability that exists in their products. CVE-2026-104286: An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] and Improper Neutralization of NULL Byte or NULL Character [CWE-158] vulnerability may allow an unauthenticated attacker to write arbitrary files on the underlying system via crafted HTTP or HTTPS requests. Fortinet advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	- FortiMail 8.0.0 through 8.0.1 - FortiMail 7.6.0 through 7.6.6 - FortiMail 7.4.0 through 7.4.8 - FortiMail 7.2.0 through 7.2.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-175

Vendor	WatchGuard
Severity	Critical
Affected Vulnerability	Missing Authentication Vulnerability (CVE-2026-13043)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. CVE-2026-13043: A missing authentication vulnerability in the Kernel Memory Access Driver (PSKMAD) used by WatchGuard endpoint security products allows a local, authenticated attacker to bypass the driver's access-control handshake and issue arbitrary privileged commands to the driver, resulting in disclosure of kernel and process memory. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Endpoint Security: Windows - Versions Prior to 8.00.26.0012
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-13043/

Vendor	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45337, CVE-2025-22869, CVE-2025-47913, CVE-2026-39827, CVE-2026-39828, CVE-2026-39829, CVE-2026-39830, CVE-2026-39831, CVE-2026-39832, CVE-2026-39833, CVE-2026-39834, CVE-2026-39835, CVE-2026-42508, CVE-2026-46595, CVE-2026-46597, CVE-2026-46598, CVE-2024-51744, CVE-2025-30204, CVE-2024-24786, CVE-2026-39821, CVE-2026-33814, CVE-2026-25680, CVE-2025-22870, CVE-2025-22872, CVE-2026-86360, CVE-2026-86361, CVE-2026-86362, CVE-2026-63697, CVE-2026-71168)
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	- Container storage modules - Versions prior to 1.17.0 - Dell System Update (DSU) - Versions prior to 2.3.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000515843/dsa-2026-324-security-update-for-dell-system-update-dsu-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000515771/dsa-2026-448-security-update-for-dell-container-storage-modules-multiple-vulnerabilities

Vendor	IBM
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-59309, CVE-2026-59310, CVE-2026-47876)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. CVE-2026-59309: VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system. CVE-2026-59310: VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code. CVE-2026-47876: VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Cloud Pak System 2.3.6.0 & 2.3.6.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288405

Vendor	Red Hat
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-45856, CVE-2026-63794, CVE-2026-80775, CVE-2022-49670, CVE-2024-57990, CVE-2026-31663, CVE-2026-43493, CVE-2026-52924, CVE-2026-53091, CVE-2026-53002, CVE-2026-52993, CVE-2026-53239, CVE-2026-63921, CVE-2026-63919, CVE-2026-63917, CVE-2026-68480, CVE-2026-64558, CVE-2026-68294, CVE-2026-68426, CVE-2026-72098, CVE-2026-74746, CVE-2026-55276, CVE-2026-53434, CVE-2026-59083, CVE-2026-65183, CVE-2026-65182, CVE-2026-65927, CVE-2026-68763, CVE-2026-68525, CVE-2026-66299, CVE-2026-73180, CVE-2026-66422, CVE-2026-68569, CVE-2026-65905, CVE-2026-45447, CVE-2026-34181, CVE-2026-34180)
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 9 Base: - Base & CodeReady Linux Builder 9 (aarch64, ppc64le, s390x, x86_64) Red Hat Enterprise Linux 9.6: 4 Years of Updates (aarch64, s390x) - Advanced Update Support (AUS) (x86_64) - CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) - Extended Update Support (EUS) (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle (ELC) (aarch64, ppc64le, s390x, x86_64) - Update Services for SAP Solutions (E4S) (ppc64le, x86_64) Red Hat Enterprise Linux 9.8: 4 Years of Updates (aarch64, s390x) - CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) - Extended Update Support (EUS) (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle (ELC) (aarch64, ppc64le, s390x, x86_64) - Update Services for SAP Solutions (E4S) (ppc64le, x86_64) Red Hat Middleware & Application Platforms: - JBoss Enterprise Web Server Text-Only Advisories (x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:74438 https://access.redhat.com/errata/RHSA-2026:74174 https://access.redhat.com/errata/RHSA-2026:73982

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
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	IBM Cloud Pak System 2.3.6.0 & 2.3.6.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	- https://www.ibm.com/support/pages/node/7288405 - https://www.ibm.com/support/pages/node/7290255 - https://www.ibm.com/support/pages/node/7290184 - https://www.ibm.com/support/pages/node/7290183

Vendor	Apache HTTP Server
Severity	Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42356, CVE-2026-42528, CVE-2026-46729, CVE-2026-47360, CVE-2026-48005, CVE-2026-56153, CVE-2026-56154, CVE-2026-56449, CVE-2026-57941, CVE-2026-58415, CVE-2026-59685, CVE-2026-59797, CVE-2026-63045, CVE-2026-63292, CVE-2026-63686, CVE-2026-63718, CVE-2026-73636, CVE-2026-73637, CVE-2026-79768, CVE-2026-93546, CVE-2026-59797, CVE-2026-57941, CVE-2026-56449)
Description	Apache HTTP Server 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. Apache HTTP Server advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Apache HTTP Server Versions - 2.4.0 through 2.4.68
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Vendor	F5
Severity	Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6469, CVE-2026-6471, CVE-2026-6470)
Description	F5 has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2026-6469: Incorrect ownership assignment in PostgreSQL ALTER TABLE ALTER TYPE command reassigns ownership of dependent statistics objects to the current user. This wrongly allows the table owner to run DROP STATISTICS and ALTER STATISTICS via this improper ownership. It wrongly denies those commands to the prior statistics object owner. DROP TABLE remains able to remove statistics objects, so this exploit achieves nothing in many ownership arrangements CVE-2026-6471: Missing authorization in PostgreSQL logical decoding allows a non-superuser holding REPLICATION privilege to dlopen any file visible to the operating system account running the server, via the choice of logical decoding plugin. This in turn runs arbitrary code as that account. CVE-2026-6470: Missing authorization in PostgreSQL DDL commands allows an object creator to achieve denial of service against ALTER and DROP of the type, via creating a dependency on the type. Many DDL operations did check the privilege, but assigning a range subtype and referencing the type from an SQL expression did not. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes - Versions: 2.3.0 - 2.3.3 2.2.0 - 2.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	- https://my.f5.com/manage/s/article/K000163494 - https://my.f5.com/manage/s/article/K000163505 - https://my.f5.com/manage/s/article/K000163496

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.