Advisory Alert

Alert Number: AAA20260520 **Date:** May 20, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Arbitrary Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
F5	**Critical**	NGINX JavaScript Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
HPE	**High**	Privilege Escalation Vulnerability
Dell	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Hitachi	**High**, Medium	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2026-42945)
Description	Red Hat has released security updates addressing a vulnerability that exists in their products. **CVE-2026-42945**: NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.8 aarch64 • Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 • Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.8 s390x • Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x • Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.8 ppc64le • Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le • Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.8 x86_64 • Red Hat CodeReady Linux Builder for x86_64 9 x86_64 • Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.8 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.8 aarch64 • Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.8 aarch64 • Red Hat Enterprise Linux for ARM 64 9 aarch64 • Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.8 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.8 s390x • Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.8 s390x • Red Hat Enterprise Linux for IBM z Systems 9 s390x • Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le • Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le • Red Hat Enterprise Linux for Power, little endian 9 ppc64le • Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 • Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64 • Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64 • Red Hat Enterprise Linux for x86_64 9 x86_64 • Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:19374 • https://access.redhat.com/errata/RHSA-2026:19371 • https://access.redhat.com/errata/RHSA-2026:19372

Affected Product	**Dell**
Severity	**Critical**
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 security fixes at your earliest to protect systems from potential threats.
Affected Products	SmartFabric Storage Software versions prior to 1.4.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000466942/dsa-2026-235-security-update-for-dell-networking-smartfabric-storage-software-vulnerabilities

Affected Product	**F5**
Severity	**Critical**
Affected Vulnerability	NGINX JavaScript Vulnerability (CVE-2026-8711)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-8711**: NGINX JavaScript has a vulnerability when the js_fetch_proxy directive is configured with at least one client-controlled NGINX variable (for example, $http_*, $arg_*, $cookie_*) and a location invoking the ngx.fetch() operation from NGINX JavaScript. An unauthenticated attacker can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX JavaScript (njs) versions 0.9.4 to 0.9.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000161307

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38024, CVE-2026-23191, CVE-2026-23243, CVE-2026-23401, CVE-2026-31419, CVE-2026-31532, CVE-2026-46300, CVE-2026-46333)
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 Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux Server - TUS 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:19521

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2026-31431)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-31431**: In the Linux kernel, the following vulnerability has been resolved: crypto: algif_aead - Revert to operating out-of-place This mostly reverts commit 72548b093ee3 except for the copying of the associated data. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Aruba Networking Management Software (Airwave) 8.3.0.6 and below. HPE Aruba Networking AOS-CX : • AOS-CX 10.17.xxxx: AOS-CX 10.17.1010 and below • AOS-CX 10.16.xxxx: AOS-CX 10.16.1040 and below • AOS-CX 10.13.xxxx: AOS-CX 10.13.1170 and below HPE Aruba Networking EdgeConnect Orchestrator HPE Aruba Networking Analytics and Location Engine (ALE)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05059en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-50181, CVE-2025-66418, CVE-2026-21441, CVE-2025-69277, CVE-2026-23490, CVE-2025-4516, CVE-2025-8291, CVE-2025-11468, CVE-2025-13837, CVE-2025-15282, CVE-2026-1299, CVE-2025-6069, CVE-2025-6075, CVE-2025-8194, CVE-2025-12084, CVE-2026-0672, CVE-2026-22695, CVE-2026-22801, CVE-2026-25646, CVE-2026-33416, CVE-2026-33636, CVE-2025-9820, CVE-2025-14831)
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 Networking OS10 versions prior to 10.5.6.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000466930/dsa-2026-161-security-update-for-dell-networking-os10-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu versions: • 14.04 LTS • 16.04 LTS • 18.04 LTS • 20.04 LTS • 22.04 LTS • 24.04 LTS • 25.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8281-1 • https://ubuntu.com/security/notices/USN-8280-1 • https://ubuntu.com/security/notices/USN-8279-1 • https://ubuntu.com/security/notices/USN-8278-1 • https://ubuntu.com/security/notices/USN-8277-1 • https://ubuntu.com/security/notices/USN-8255-3 • https://ubuntu.com/security/notices/USN-8274-1 • https://ubuntu.com/security/notices/USN-8273-1

Affected Product	**Hitachi**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23667, CVE-2026-23668, CVE-2026-23669, CVE-2026-23671, CVE-2026-23672, CVE-2026-23673, CVE-2026-23674, CVE-2026-24282, CVE-2026-24285, CVE-2026-24287, CVE-2026-24288, CVE-2026-24289, CVE-2026-24290, CVE-2026-24291, CVE-2026-24292, CVE-2026-24293, CVE-2026-24294, CVE-2026-24295, CVE-2026-24296, CVE-2026-24297, CVE-2026-25165, CVE-2026-25166, CVE-2026-25168, CVE-2026-25169, CVE-2026-25171, CVE-2026-25173, CVE-2026-25174, CVE-2026-25175, CVE-2026-25176, CVE-2026-25177, CVE-2026-25178, CVE-2026-25179, CVE-2026-25180, CVE-2026-25181, CVE-2026-25185, CVE-2026-25186, CVE-2026-25187, CVE-2026-25188, CVE-2026-25189, CVE-2026-25190, CVE-2026-26128, CVE-2026-26132)
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 5200, 5600, 5200H, 5600H Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/03.html

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4410, CVE-2026-5516)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-4410**: IBM WebSphere Application Server and WebSphere Application Server Liberty are vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. **CVE-2026-5516**: IBM WebSphere Application Server Liberty could allow a remote attacker to bypass security under limited conditions by exploiting a specific timing window. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM WebSphere Application Server - Liberty versions 19.0.0.7 to 26.0.0.5 IBM WebSphere Application Server version 9.0 IBM WebSphere Application Server version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7273424 • https://www.ibm.com/support/pages/node/7273425

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.