Advisory Alert

Alert Number: AAA20260903 **Date:** September 3, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Improper TLS Certificate Validation Vulnerability
HPE	**High**, **Medium**	Multiple Vulnerabilities
Drupal	**High**, **Medium**	Multiple Vulnerabilities
F5	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20274, CVE-2026-20275, CVE-2026-20276, CVE-2026-20277, CVE-2026-20278, CVE-2026-20279, CVE-2026-20280, CVE-2026-20212)
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 IOS XR Software versions: • 7.3, 7.9, 7.10, and 7.11 • 24.1, 24.2, 24.3 and 24.4 • 25.1, 25.2, and 25.4 • 26.1, 26.2, 26.3 Cisco Nexus 9000 Series Switches (if they include a Silicon One ASIC)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-n9k-s1-rce-EH8dEtr • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxr-qg64NcM

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16439, CVE-2026-16441)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-16439:** In Eclipse OpenJ9 versions up to 0.60, using -Xtrace to trace method arguments can lead to buffer underflow. **CVE-2026-16441:** In Eclipse OpenJ9 versions up to 0.60, when executing class files where a previously concrete superclass method has been recompiled as abstract, execution is incorrectly delegated to an interface default method. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security SOAR versions 51.0.10, 51.0.9, 51.0.8, 51.0.7, 51.0.6 IBM Verify Identity Access versions: • 11.0.0 - 11.0.3 IF1 • 10.0.0 - 10.0.9.2 IF1 IBM Verify Identity Access Container versions: • 11.0.0 - 11.0.3 IF1 • 10.0.0 - 10.0.9.2 IF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286058 https://www.ibm.com/support/pages/node/7286188

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-57849, CVE-2025-71132, CVE-2026-45970, CVE-2026-53185, CVE-2026-63800, CVE-2026-53397, CVE-2026-53399, CVE-2026-53392, CVE-2026-53391, CVE-2026-64018, CVE-2026-64268, CVE-2026-64298, CVE-2026-68480, CVE-2026-74581, CVE-2022-4318, CVE-2026-15809, CVE-2026-34986, CVE-2026-23111, CVE-2026-43114, CVE-2026-43112, CVE-2026-46323, CVE-2026-53264, CVE-2026-52973, CVE-2026-46150, CVE-2026-46120, CVE-2026-53361, CVE-2026-64002, CVE-2026-74480, CVE-2024-46744, CVE-2025-68211, CVE-2026-43023, CVE-2026-46099, CVE-2026-46056, CVE-2026-46145, CVE-2026-53006, CVE-2026-64304, CVE-2026-74580)
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 8 (base) — x86_64, s390x, ppc64le, aarch64 • RHEL 8 CodeReady Linux Builder — x86_64, ppc64le, aarch64 • RHEL 8.8 — Extended Life Cycle Long Life (x86_64); Update Services for SAP Solutions (x86_64, ppc64le) • RHEL 8.10 — Extended Life Cycle (x86_64, ARM64, ppc64le, s390x) • RHEL 9 (base) — x86_64, ppc64le • RHEL 9.2 — AUS (x86_64); SAP (x86_64, ppc64le); Extended Life Cycle (x86_64, ARM64, ppc64le, s390x); 4 years of updates (ARM64, s390x) • RHEL 9.4 — AUS (x86_64); SAP (x86_64, ppc64le); Extended Life Cycle (x86_64, ppc64le) • RHEL 9.6 — EUS (x86_64, ppc64le, s390x, ARM64); AUS (x86_64); SAP (x86_64, ppc64le); Extended Life Cycle (x86_64, ppc64le, ARM64, s390x); 4 years of updates (ARM64, s390x); CodeReady Linux Builder EUS (x86_64, ppc64le, s390x, ARM64) • RHEL 9.8 — EUS (x86_64, ppc64le); SAP (x86_64, ppc64le); Extended Life Cycle (x86_64, ppc64le) • RHEL 10 (base) — x86_64, ppc64le • RHEL 10.0 — EUS (x86_64, s390x, ppc64le, ARM64); 4 years of updates (x86_64, s390x, ppc64le, ARM64); CodeReady Linux Builder EUS (x86_64, ppc64le, s390x, ARM64) • RHEL 10.2 — EUS (x86_64, ppc64le); 4 years of updates (x86_64); 4 years of support (ppc64le); Extended Life Cycle (x86_64, ppc64le) • OpenShift Container Platform 4.19 — RHEL 9 only, all architectures (x86_64, ppc64le, s390x, aarch64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:63014 https://access.redhat.com/errata/RHSA-2026:60452 https://access.redhat.com/errata/RHSA-2026:62641 https://access.redhat.com/errata/RHSA-2026:62642 https://access.redhat.com/errata/RHSA-2026:62641 https://access.redhat.com/errata/RHSA-2026:62640 https://access.redhat.com/errata/RHSA-2026:62639 https://access.redhat.com/errata/RHSA-2026:62638 https://access.redhat.com/errata/RHSA-2026:62609 https://access.redhat.com/errata/RHSA-2026:62568 https://access.redhat.com/errata/RHSA-2026:62558 https://access.redhat.com/errata/RHSA-2026:62508

Vendor	**Dell**
Severity	**High**
Affected Vulnerability	Improper TLS Certificate Validation Vulnerability (CVE-2026-68864)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-68864:** Dell Open Manage Python SDK (omsdk) contains an improper TLS certificate validation issue in the redfish_operation execution path. The SDK exposes a verify_ssl configuration option intended to control certificate validation. However, WsManProtocolBase.redfish_operation ignores this setting and unconditionally disables certificate validation by passing verify=False to the underlying HTTP request. As a result, an operator explicitly enabling TLS verification with verify_ssl=True still performs Redfish communication without certificate validation. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Open Manage Python SDK (omsdk) versions 1.2.519
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000505139/dsa-2026-358-security-update-for-dell-openmanage-python-sdk-omsdk-vulnerability

Vendor	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6727, CVE-2026-6726, CVE-2026-20707)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2026-6727: A potential security vulnerability in HPE ProLiant DL/ML/XL, Alletra, Apollo, Edgeline, and Synergy servers using certain Intel processors could be locally exploited to allow escalation of privilege vulnerability. **CVE-2026-6726**: A potential security vulnerability in HPE ProLiant DL/ML/XL, Alletra, Apollo, MicroServer, Edgeline, and Synergy servers using certain Intel processors could be locally exploited to allow escalation of privilege vulnerability. **CVE-2026-20707**: A potential security vulnerability in HPE ProLiant DL/ML/XL, Alletra, Apollo, MicroServer, Edgeline, and Synergy servers using certain Intel processors could be locally exploited to allow escalation of privilege vulnerability. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05087en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05088en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05118en_us&docLocale=en_US

Vendor	**Drupal**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84920, CVE-2026-84918, CVE-2026-81163, CVE-2026-84917, CVE-2026-84924, CVE-2026-84923)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Unpublished Node Permissions module versions prior to 1.8.0 Monobank payment API module versions prior to 1.0.3 Media Library Importer module versions prior to 2.1.6 Jsonapi Role Access module versions prior to 2.0.2 OTP Verification module versions prior to 2.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-132 https://www.drupal.org/sa-contrib-2026-130 https://www.drupal.org/sa-contrib-2026-129 https://www.drupal.org/sa-contrib-2026-127 https://www.drupal.org/sa-contrib-2026-125 https://www.drupal.org/sa-contrib-2026-124

Vendor	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20068, CVE-2026-66362, CVE-2026-78689, CVE-2026-66842, CVE-2026-77180)
Description	F5 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. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	F5OS version 2.0.0 (VELOS systems) F5OS-A versions 1.8.0 - 1.8.3 and 1.5.1 - 1.5.4 NGINX Gateway Fabric version 2.5.0 - 2.6.7 NGINX JavaScript version 1.0.0 BIG-IP (all modules) versions: • 21.0.0 - 21.1.0 • 17.5.0 - 17.5.1 and 17.1.0 - 17.1.3 BIG-IQ version 8.4.0 - 8.4.2 NGINX Ingress Controller versions: • 2026-lts-r1 - 2026-lts-r4 • 5.0.0 - 5.5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000163165 https://my.f5.com/manage/s/article/K000162600 https://my.f5.com/manage/s/article/K000162602 https://my.f5.com/manage/s/article/K000162521 https://my.f5.com/manage/s/article/K000162601

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-41254, CVE-2026-47057, CVE-2026-47063, CVE-2026-47058, CVE-2026-60147, CVE-2026-46968, CVE-2026-47027, CVE-2026-47021, CVE-2026-47059, CVE-2026-47010, CVE-2026-8400, CVE-2026-16243, CVE-2026-11927, CVE-2026-12358, CVE-2026-11934, CVE-2026-11921, CVE-2026-11928, CVE-2026-11932, CVE-2026-12101, CVE-2026-11929, CVE-2026-14981, CVE-2026-15064, CVE-2026-15328, CVE-2026-15325, CVE-2026-13297, CVE-2026-13276, CVE-2026-13260, CVE-2026-11926, CVE-2026-13277, CVE-2026-13272)
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 Security SOAR versions 51.0.10, 51.0.9, 51.0.8, 51.0.7, 51.0.6 IBM Verify Identity Access versions: • 11.0.0 - 11.0.3 IF1 • 10.0.0 - 10.0.9.2 IF1 IBM Verify Identity Access Container versions: • 11.0.0 - 11.0.3 IF1 • 10.0.0 - 10.0.9.2 IF1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7286058 https://www.ibm.com/support/pages/node/7286188

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-64531, CVE-2026-53359, CVE-2026-53246, CVE-2026-53228, CVE-2026-53225, CVE-2026-53224, CVE-2026-53215, CVE-2026-53212, CVE-2026-53176, CVE-2026-53086, CVE-2026-52989, CVE-2026-52924, CVE-2026-46331, CVE-2026-46266, CVE-2026-43499, CVE-2026-43378, CVE-2026-43198, CVE-2026-31705, CVE-2026-31448, CVE-2026-31414, CVE-2025-27558, CVE-2026-53309, CVE-2026-53043)
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 18.04 and 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8661-4 https://ubuntu.com/security/notices/USN-8714-1

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.