Advisory Alert

Alert Number: AAA20260915 **Date:** September 15, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Allocation of Resources Without Limits Vulnerability

Description

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76461, CVE-2026-20353, CVE-2026-76440, CVE-2026-76441, CVE-2026-76442, CVE-2026-76443)
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 Secure Email Gateway & Cisco Secure Email and Web Manager Versions: • 15.5 and earlier • 16.0 • 16.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-inj-2bLVGmhX • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-52933, CVE-2026-53196, CVE-2026-64387, CVE-2026-64530, CVE-2026-74480, CVE-2026-3012, CVE-2026-6893, CVE-2026-15816, CVE-2026-42010, CVE-2026-43112, CVE-2026-2340, CVE-2026-3833, CVE-2026-14164, CVE-2026-29111, CVE-2024-53161, CVE-2025-71127, CVE-2026-43133, CVE-2026-52947, CVE-2026-53182, CVE-2026-63802, CVE-2026-63889, CVE-2026-64117, CVE-2026-68363, CVE-2026-72098, CVE-2026-74556)
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 for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat OpenShift Container Platform 4.14 for RHEL 9 x86_64 Red Hat OpenShift Container Platform 4.14 for RHEL 8 x86_64 Red Hat OpenShift Container Platform for Power 4.14 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for Power 4.14 for RHEL 8 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 9 s390x Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.14 for RHEL 8 s390x Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 9 aarch64 Red Hat OpenShift Container Platform for ARM 64 4.14 for RHEL 8 aarch64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:67114 • https://access.redhat.com/errata/RHSA-2026:67277 • https://access.redhat.com/errata/RHSA-2026:62409 • https://access.redhat.com/errata/RHSA-2026:67468

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16190, CVE-2026-15887, CVE-2026-15412, CVE-2026-16435, CVE-2026-15396, CVE-2026-15634, CVE-2026-16185, CVE-2026-10841, CVE-2026-11548, CVE-2026-11549, CVE-2026-11722, CVE-2026-9327, CVE-2026-9667, CVE-2026-9338, CVE-2026-16188, CVE-2026-9176, CVE-2026-11540, CVE-2026-11539, CVE-2026-11538, CVE-2026-11711, CVE-2026-16186, CVE-2026-16187, CVE-2026-11537, CVE-2026-16189, CVE-2026-9336, CVE-2026-11710, CVE-2026-16440, CVE-2026-61308, CVE-2026-70907, CVE-2026-60589, CVE-2026-11545)
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	WebSphere Service Registry and Repository - Version 8.5 - 8.5.6.3 WebSphere Service Registry and Repository Studio - Version 8.5 - 8.5.6.3 WebSphere Application Server – Versions 8.5 & 9.0 WebSphere Application Server - Liberty - Continuous delivery
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7286610 • https://www.ibm.com/support/pages/node/7287333 • https://www.ibm.com/support/pages/node/7287432 • https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-privilege-escalation-cve-2026-11545 • https://www.ibm.com/support/pages/security-bulletin-ibm-websphere-application-server-affected-http-request-smuggling-vulnerability-cve-2026-11710

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Allocation of Resources Without Limits Vulnerability (CVE-2026-60001)
Description	Dell has released a security update addressing a vulnerability that exist in their products. **CVE-2026-60001:** CVE-2026-60001 affects sshd in OpenSSH versions before 10.4. The daemon does not always honor the configured minimum authentication delay. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC9 - Versions prior to 7.30.30.54 iDRAC10 - Versions prior to 1.30.40.51
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000509006/dsa-2026-415-security-update-for-dell-idrac9-and-idrac10-vulnerability

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.