Advisory Alert

Alert Number: AAA20260806 **Date:** August 6, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Denial of Service Vulnerability
Drupal	**Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Client-Side Memory Leak Vulnerability

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-16242, CVE-2026-33186, CVE-2026-40895, CVE-2026-42154, CVE-2026-4800, CVE-2026-9277)
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 OpenShift Container Platform
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:48657 https://access.redhat.com/errata/RHSA-2026:48699

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-4408, CVE-2026-4480, CVE-2026-41293, CVE-2026-43037, CVE-2026-43038, CVE-2026-43125, CVE-2026-31669, CVE-2026-23455, CVE-2026-31685, CVE-2026-42496, CVE-2026-43512, CVE-2026-43515)
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar versions 7.5.0 through 7.5.0 UP15 IF04 and 7.6.0.0 through 7.6.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7282618

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20303, CVE-2026-20304, CVE-2026-20310, CVE-2026-20312, CVE-2026-20313, CVE-2026-20267, CVE-2026-20268, CVE-2026-20269, CVE-2026-20270, CVE-2026-20271, CVE-2026-20272, CVE-2026-20273, CVE-2026-20079)
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 Catalyst SD-WAN Software (All Deployment Types) Cisco IOS XE Software Cisco Secure FMC Software Cisco Security Cloud Control (SCC) Firewall Management
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53404, CVE-2026-53434, CVE-2026-55276, CVE-2026-59083, CVE-2026-25681, CVE-2026-27136, CVE-2026-33186, CVE-2026-33811, CVE-2026-39820, CVE-2026-39821, CVE-2026-42151, CVE-2026-42154, CVE-2026-42499, CVE-2026-42504)
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	Logging Subsystem for Red Hat OpenShift JBoss Enterprise Web Server 7 (RHEL 8, 9, 10): x86_64 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-2026:50843 https://access.redhat.com/errata/RHSA-2026:49951 https://access.redhat.com/errata/RHSA-2026:49952

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20198, CVE-2026-20289, CVE-2026-20294, CVE-2026-20028, CVE-2026-20308, CVE-2026-20311, CVE-2026-20316, CVE-2026-20200, CVE-2026-20288, CVE-2026-20301, CVE-2026-20263, CVE-2026-20124)
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 Integrated Management Controller (IMC): • 5000 Series Enterprise Network Compute Systems (ENCS) • Catalyst 8300 Series Edge uCPE • UCS C-Series M5, M6, M7, and M8 Rack Servers in standalone mode • UCS E-Series Servers M3 • UCS E-Series Servers M6 • UCS S-Series Storage Servers in standalone mode Cisco RoomOS Cisco Catalyst SD-WAN Manager (All Deployment Types) Cisco TS Agent Cisco Secure FMC Software Cisco IOS and IOS XE Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-7EhBFxBp • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-roomos-infodisc-qBXjfmWm • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-infodis-SPuJBDCe • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ts-agent-fw-bypass-MYBTMrev • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-dos-qdc7qx3 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-webui-dos-PtAODAWW • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xmcp-thbAr34t • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-bing-MGHrFAkd • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-snmp-dos-ZAqNm4MD

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM 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. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	QRadar versions 7.5.0 through 7.5.0 UP15 IF04 and 7.6.0.0 through 7.6.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7282618

Vendor	**HPE**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-63457)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-63457:** A potential security vulnerability has been identified in HPE Integrated Lights-out 6 (iLO 6). The vulnerability could be remotely exploited to allow denial of service. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Integrated Lights-Out 6 (iLO 6) - Prior to v1.78
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05090en_us&docLocale=en_US

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-18986, CVE-2026-18985)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-18986:** The Entity Browser module doesn't sufficiently sanitize the the tab titles, resulting in a stored cross-site scripting (XSS) vulnerability. **CVE-2026-18985:** The Edit in-place field module doesn't sufficiently check access when editing entities. A malicious user could craft requests to allow them to modify any field on any entity. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Edit in-place field module versions prior to 2.1.1 Entity Browser module versions prior to Entity Browser 8.x-2.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-094 https://www.drupal.org/sa-contrib-2026-093

Vendor	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Client-Side Memory Leak Vulnerability (CVE-2026-54876)
Description	OpenSSL has released a security update addressing a vulnerability that exists in their products. **CVE-2026-54876:** A malicious TLS server can cause a memory leak in a TLS client that has enabled OCSP response checking by sending an OCSP response that contains no single response entries. An attacker can leak an attacker-tunable amount of memory per TLS handshake in a victim client application. A long-running client that repeatedly connects to a malicious server can have its memory exhausted, resulting in a Denial of Service. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL versions: from 4.0.0 before 4.0.2 from 3.6.0 before 3.6.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/#CVE-2026-54876

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.