



Advisory Alert

Alert Number: AAA20261008 Date: October 8, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Drupal	Critical	PHP Object Injection Vulnerability
Cisco	Critical	Multiple Vulnerabilities
IBM	Critical	Input Validation Vulnerability
Red Hat	High	Multiple Vulnerabilities
Drupal	High, Medium	Multiple Vulnerabilities
Cisco	High, Medium	Multiple Vulnerabilities
cPanel	High, Medium, Low	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities

Description

Vendor	Drupal
Severity	Critical
Affected Vulnerability	PHP Object Injection Vulnerability (CVE-2026-107249)
Description	Drupal has released a security update addressing a vulnerability that exists in their products. CVE-2026-107249: The module doesn't sufficiently validate user-supplied data which is used to construct a block. In the worst case scenario, this can lead to PHP Object Injection and Remote Code Execution. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Block AJAX versions prior to 3.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-192

Vendor	Cisco
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20328, CVE-2026-76437, CVE-2026-76452, CVE-2026-76454, CVE-2026-76485, CVE-2026-76486, CVE-2026-76501, CVE-2026-76471, CVE-2026-76465, CVE-2026-76480, CVE-2026-76482, CVE-2026-76483, CVE-2026-76484, CVE-2026-76453, CVE-2026-76455, CVE-2026-76456, CVE-2026-76457, CVE-2026-76458, CVE-2026-76459, CVE-2026-76498, CVE-2026-76499, CVE-2026-76500)
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 License On-Prem Cisco Nexus 3000 Series Switches Cisco Nexus 7000 Series Switches Cisco Nexus 9000 Series Switches in standalone NX-OS mode Cisco Nexus 9000 Series Fabric Switches in ACI mode UCS 6300 Series Fabric Interconnects UCS 6400 Series Fabric Interconnects UCS 6500 Series Fabric Interconnects UCS 6600 Series Fabric Interconnects UCS X-Series Direct Fabric Interconnect 9108 100G MDS 9000 Series Multilayer Switches Cisco APIC
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-access-nttb2dhE

	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngoam-rce-LWKQ4BU https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-napi-rce-r2shwu2j https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-moam-rce-uBTzYV7 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-nxosw1-cWzSbtR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh
--	--

Vendor	IBM
Severity	Critical
Affected Vulnerability	Input Validation Vulnerability (CVE-2026-34182)
Description	IBM has released a security update addressing a vulnerability that exists in their products. CVE-2026-34182: Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers, leading to various potential compromises. 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 and 2.3.6.1 IBM OS Image for Red Hat Enterprise Linux 5.0.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291507

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40026, CVE-2026-65183, CVE-2026-65637, CVE-2026-65182, CVE-2026-65927, CVE-2026-68763, CVE-2026-68525, CVE-2026-73180, CVE-2026-66299, CVE-2026-66422, CVE-2026-68569, CVE-2026-65905, CVE-2026-45447, CVE-2026-34181, CVE-2026-64115, CVE-2026-74582, CVE-2026-89530, CVE-2023-53781, CVE-2025-68347, CVE-2026-31663, CVE-2026-43020, CVE-2026-46043, CVE-2026-46133, CVE-2026-52924, CVE-2026-53239, CVE-2026-63921, CVE-2026-63919, CVE-2026-63917, CVE-2026-68480, CVE-2026-64582, CVE-2026-68294, CVE-2026-68426, CVE-2026-74746, CVE-2026-80864, CVE-2026-80863, CVE-2026-31613, CVE-2026-45910, CVE-2026-46114, CVE-2026-63924, CVE-2026-63922, CVE-2026-63920, CVE-2026-64007, CVE-2026-63984, CVE-2026-72130, CVE-2026-80792)
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 9.4 - Advanced Update Support (AUS) (x86_64) 4 Years of Updates (aarch64, s390x) - Extended Life Cycle (ELC) (aarch64, ppc64le, s390x, x86_64) - Update Services for SAP Solutions (E4S) (ppc64le, x86_64) RHEL 8 Series & Minor Releases - Base & CodeReady Linux Builder 8 (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle (ELC) 8.10 (aarch64, ppc64le, s390x, x86_64) - Extended Life Cycle Long Life 8.8 (x86_64) - Telecommunications Update Service (TUS) 8.8 (x86_64) - Update Services for SAP Solutions (E4S) 8.8 (ppc64le, x86_64) RHEL 7 Legacy - Extended Life Cycle Support (ELS) (ppc64, ppc64le, s390x, 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-2026:78844 https://access.redhat.com/errata/RHSA-2026:76956 https://access.redhat.com/errata/RHSA-2026:77498 https://access.redhat.com/errata/RHSA-2026:77301 https://access.redhat.com/errata/RHSA-2026:77218

Vendor	Drupal
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-107262, CVE-2026-107255, CVE-2026-107311, CVE-2026-107310, CVE-2026-107309, CVE-2026-107308, CVE-2026-107307, CVE-2026-107306, CVE-2026-107267, CVE-2026-107268, CVE-2026-96389, CVE-2026-107266, CVE-2026-107265, CVE-2026-107264, CVE-2026-107263, CVE-2026-107261, CVE-2026-107259, CVE-2026-107258, CVE-2026-107257, CVE-2026-107254, CVE-2026-107253, CVE-2026-107252, CVE-2026-107251, CVE-2026-107250)
Description	Drupal 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. Drupal 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://www.drupal.org/security

Vendor	Cisco
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20362, CVE-2026-20173, CVE-2026-20032, CVE-2026-76488, CVE-2026-20321, CVE-2026-20038)
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 Finesse Packaged Contact Center Enterprise (Packaged CCE) Unified Contact Center Enterprise (Unified CCE) Unified Contact Center Express (Unified CCX) Cisco Nexus 3000 Series Switches Cisco Nexus 7000 Series Switches Cisco Nexus 9000 Series Switches in standalone NX-OS mode MDS 9000 Series Multilayer Switches Cisco APIC
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-ssrf-mmSuyugS https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-nscpdos-SnderkC7 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-mppe-dhKZAFgb https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-info-priv-enAdB5vD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apic-cmdinj-L6VR4E7 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-epgcbp-SfDU7Nlf

Vendor	cPanel
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-61812, CVE-2026-61813, CVE-2026-73857, CVE-2026-104259, CVE-2026-104269, CVE-2026-84782, CVE-2026-35189, CVE-2026-54872, CVE-2026-75806, CVE-2026-77696, CVE-2022-24836, CVE-2022-29181)
Description	cPanel 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. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	ea-apache24-mod_security2 versions prior to 2.9.15 ea-openssl11 ea-ruby27-rubygem-nokogiri versions prior to 1.15.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-68497, CVE-2018-1000665, CVE-2026-34477, CVE-2026-34478, CVE-2026-34479, CVE-2026-34480, CVE-2026-54512, CVE-2026-54513, CVE-2026-54514, CVE-2026-54515, CVE-2026-54399, CVE-2026-49844, CVE-2026-59888, CVE-2026-66142, CVE-2026-66143, CVE-2026-66144, CVE-2026-77310, CVE-2026-18401, CVE-2026-68494, CVE-2026-83557, CVE-2020-5258, CVE-2026-42402, CVE-2026-42403, CVE-2026-42404, CVE-2026-91776, CVE-2026-91777, CVE-2026-89407, CVE-2026-89425, CVE-2026-19032, CVE-2026-34181, CVE-2026-7383, CVE-2026-34180, CVE-2026-34183, CVE-2026-42764, CVE-2026-42766, CVE-2026-42767, CVE-2026-42768, CVE-2026-42769, CVE-2026-42770, CVE-2026-45445, CVE-2026-45446, CVE-2026-45447, CVE-2026-9076)
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	InfoSphere Data Architect 9.2.1 IBM Cloud Pak System 2.3.6.0 and 2.3.6.1 IBM OS Image for Red Hat Enterprise Linux 5.0.2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291516 https://www.ibm.com/support/pages/node/7291507

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.