AAA20260716.pdf

Advisory Alert

Alert Number: AAA20260716 **Date:** July 16, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Cross Site Scripting Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Nginx	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
F5	**High**, Medium	Multiple Vulnerabilities
Lenovo	**High**, Medium	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities
Ivanti	**Medium**	Improper Authorization Vulnerability

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Cross Site Scripting Vulnerabilities (CVE-2026-11712, CVE-2026-11708)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-11712:** BM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console help system. **CVE-2026-11708:** IBM WebSphere Application Server 9.0, and 8.5 is affected by a cross-site scripting vulnerability in the administrative console's integrated help system. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WebSphere Service Registry and Repository - Versions 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7280105

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43027, CVE-2026-43499, CVE-2026-46113, CVE-2026-53166, CVE-2026-53359, CVE-2025-68183, CVE-2026-31613, CVE-2026-31684, CVE-2026-46189, CVE-2026-46209, CVE-2026-46135)
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 Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.2 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.6 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.6 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.6 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:40082 https://access.redhat.com/errata/RHSA-2026:40068 https://access.redhat.com/errata/RHSA-2026:39984 https://access.redhat.com/errata/RHSA-2026:40425

Vendor	**Dell**
Severity	**High**
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 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.dell.com/support/kbdoc/en-us/000489640/dsa-2026-300-security-update-for-dell-thinos-10-for-multiple-vulnerabilities

Vendor	**Nginx**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42533, CVE-2026-60005, CVE-2026-56434)
Description	Nginx has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-42533:** A vulnerability exists in NGINX Plus and NGINX Open Source when a map directive uses regex matching and a string expression references the map's regex capture variables before referencing the map output variable. An unauthenticated attacker along with conditions beyond their control 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, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. **CVE-2026-56434:** NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_slice_module module. When the slice directive and unnamed regex captures are configured or when a background cache update happens, unauthenticated attackers can send requests that may cause uninitialized memory access in the NGINX worker process, leading to limited disclosure of memory or a restart. **CVE-2026-60005:** NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_ssi_module module. This vulnerability may exist when the Server-Side Includes (SSI), proxy_pass, and proxy_buffering off directives are configured. With this configuration, an unauthenticated attacker with man-in-the-middle (MITM) ability to control responses from an upstream server may be able to cause a use-after-free in the NGINX worker process. nginx advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NGINX Plus - Versions 37.0.0.1 - 37.0.2.1 & R33 - R36 NGINX Open Source - Versions 1.31.2 & 1.30.0 - 1.30.3 NGINX Gateway Fabric – Versions 2.0.0 - 2.6.6 & 1.3.0 - 1.6.2 NGINX Ingress Controller – Versions 2026-lts-r1 - 2026-lts-r3 & 5.0.0 - 5.5.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162097 https://my.f5.com/manage/s/article/K000162100 https://my.f5.com/manage/s/article/K000162098

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-31758, CVE-2026-43037, CVE-2026-43501, CVE-2026-45970, CVE-2026-46120, CVE-2026-46173, CVE-2026-46227, CVE-2026-46243, CVE-2026-52909, CVE-2026-52943, CVE-2026-53362, CVE-2026-43366, CVE-2026-31685, CVE-2026-43025, CVE-2026-43190, CVE-2026-43437, CVE-2026-31771, CVE-2026-43038, CVE-2026-46090, CVE-2026-46229, CVE-2026-46253, CVE-2026-46266, CVE-2026-46274, CVE-2026-46319, CVE-2026-46320, CVE-2026-46331, CVE-2026-52918, CVE-2026-52923, CVE-2026-52924, CVE-2026-52955, CVE-2026-52969, CVE-2026-52972, CVE-2026-52993, CVE-2026-53016, CVE-2026-53041, CVE-2026-53053, CVE-2026-53071, CVE-2026-53072, CVE-2026-53133, CVE-2026-53253, CVE-2026-53359)
Description	SUSE 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. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.4, 15.5, 15.6 SUSE Linux Enterprise Live Patching 15-SP4, 15-SP5, 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP4, 15 SP5, 15 SP6 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP4, SP5 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Server 15 SP4 LTSS SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 & Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20262997-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263001-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263002-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20262995-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263008-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263009-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263011-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263044-1/

Vendor	**F5**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-60065, CVE-2026-52865, CVE-2026-60062, CVE-2026-55723, CVE-2026-59762)
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	NGINX Agent - Versions 2.37.0 - 2.46.5 BIG-IP Next SPK - Versions 1.7.0 - 1.9.2 BIG-IP Next CNF • 2.0.0 - 2.3.1 • 1.1.0 - 1.4.2 BIG-IP Next for Kubernetes – Versions 2.0.0 - 2.3.1 BIG-IP (all modules) • 21.0.0 - 21.1.0 • 17.5.0 - 17.5.1 • 17.1.0 - 17.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162231 https://my.f5.com/manage/s/article/K000161800 https://my.f5.com/manage/s/article/K000161971 https://my.f5.com/manage/s/article/K000161834 https://my.f5.com/manage/s/article/K000162098 https://my.f5.com/manage/s/article/K000162101

Vendor	**Lenovo**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-10587, CVE-2026-10588, CVE-2026-10589, CVE-2026-10590, CVE-2026-25271)
Description	Lenovo 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. Lenovo 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.lenovo.com/us/en/product_security/LEN-220440

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-20146, CVE-2026-20150, CVE-2026-20153, CVE-2026-20156, CVE-2026-20157, CVE-2026-20158, CVE-2026-20187)
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 Identity Services Engine (ISE) Cisco ISE Passive Identity Connector (ISE-PIC) Cisco RoomOS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-traversal-xNt7wb2Y https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-roomos-AqNMbEq

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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	16.04, 14.04, 20.04, 14.04, 25.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8545-1 https://ubuntu.com/security/notices/USN-8546-1 https://ubuntu.com/security/notices/USN-8547-1 https://ubuntu.com/security/notices/USN-8548-1

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-50645, CVE-2026-9322, CVE-2026-9171, CVE-2026-11595, CVE-2026-8408, CVE-2026-10842, CVE-2025-2884, CVE-2025-13995, CVE-2025-36051, CVE-2025-15051, CVE-2026-1276, CVE-2025-6021, CVE-2026-6051, CVE-2026-56403, CVE-2026-56404, CVE-2026-56405, CVE-2026-56406, CVE-2026-56407, CVE-2026-56408, CVE-2026-56409, CVE-2026-56410, CVE-2026-56411, CVE-2026-56412, CVE-2026-50219, CVE-2026-56131, CVE-2026-56132, CVE-2026-45186, CVE-2026-41080)
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	WebSphere Service Registry and Repository - Versions 8.5 & 9.0 WebSphere Application Server - Liberty - Versions 17.0.0.3 - 26.0.0.7 IBM Storage Scale System Versions: • 6.2.0.0 - 6.2.3.5 • 7.0.0.0 - 7.0.0.2 QRadar - Versions 7.5.0 - 7.5.0 UP14 IF05 IBM Cloud Pak System Versions: • 2.3.4.0 • 2.3.4.1 • 2.3.4.1 IFix1 • 2.3.5.0 • 2.3.6.0 IBM® Db2® • 11.5.0 - 11.5.9 • 12.1.0 - 12.1.4 AIX - Version 7.3 VIOS - Version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/bulletin/

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-15917, CVE-2026-55805)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-15917:** Drupal core's XSS filter does not sufficiently sanitize certain HTMX attributes, which can lead to a cross-site scripting (XSS) vulnerability. **CVE-2026-55805:** The Layout Builder module doesn't sufficiently sanitize block labels in certain scenarios, which can lead to a cross-site scripting (XSS) vulnerability. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Drupal Core Module Versions: • 11.3.0 to 11.3.14 • 11.4.0 to 11.4.4 • 11.0, 11.1, 11.2 All Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-core-2026-011 https://www.drupal.org/sa-core-2026-012

Vendor	**Ivanti**
Severity	**Medium**
Affected Vulnerability	Improper Authorization Vulnerability (CVE-2026-55956)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-55956:** Improper Authorization vulnerability in Apache Tomcat leads to security constraints specified for the default servlet ignoring any method or method omission configured as part of the constraint. Ivanti advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ivanti EPMM And Sentry Apache Tomcat Versions: • 11.0.0-M1 through 11.0.22 • 10.1.0-M1 through 10.1.55 • 9.0.0.M1 through 9.0.118 • 8.5.0 through 8.5.100 • 7.0.0 through 7.0.109
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://hub.ivanti.com/s/article/EPMM-Impact-of-CVE-2026-55956-On-EPMM-And-Sentry?language=en_US

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.