Advisory Alert

Alert Number: AAA20260730 **Date:** July 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Broadcom	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Citrix	**High**	Multiple Vulnerabilities
F5	**High**	Multiple Vulnerabilities
Cisco	**High**	Static Credential Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Asus	**High**	Race Condition Vulnerability
Samba	**High**, Medium	Multiple Vulnerabilities
NodeJS	**High**, Medium, Low	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
Drupal	Medium	Access Bypass Vulnerability

Description

Vendor	**Broadcom**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-59309, CVE-2026-59310, CVE-2026-47876, CVE-2026-41703, CVE-2026-41709)
Description	Broadcom 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. Broadcom advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• VMware ESX • VMware vCenter • VMware Workstation • VMware Fusion • VMware Cloud Foundation • VMware vSphere Foundation • VMware Telco Cloud Platform • VMware Telco Cloud Infrastructure
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14446, CVE-2026-14529, CVE-2026-14512, CVE-2026-11856, CVE-2026-10536, CVE-2026-8924, CVE-2026-8927)
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	AIX - Versions 7.3 IBM WebSphere Application Server - Versions 8.5 & 9.0 IBM WebSphere Application Server Liberty Versions 17.0.0.3 - 26.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7281743 • https://www.ibm.com/support/pages/node/7281721 • https://www.ibm.com/support/pages/node/7281649 • https://www.ibm.com/support/pages/node/7281631

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-40026, CVE-2026-31787, CVE-2026-52923, CVE-2026-64600)
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 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 9.4 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.4 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 9.4 s390x Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.8 x86_64 Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 9.8 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.8 ppc64le 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 Power, little endian - Extended Update Support 9.6 ppc64le 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 Enterprise Linux for x86_64 - Extended Life Cycle 9.6 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.6 ppc64le 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 x86_64 - Extended Life Cycle 9.2 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 9.2 ppc64le Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.8 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:48386 • https://access.redhat.com/errata/RHSA-2026:47981 • https://access.redhat.com/errata/RHSA-2026:47983 • https://access.redhat.com/errata/RHSA-2026:47997 • https://access.redhat.com/errata/RHSA-2026:47998 • https://access.redhat.com/errata/RHSA-2026:48016

Vendor	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-42492, CVE-2026-62428, CVE-2026-62431, CVE-2026-62432, CVE-2026-62434, CVE-2026-62435, CVE-2026-62436)
Description	Citrix 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. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	XenServer - Versions 8.4 XenServer - Version 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696836&articleURL=XenServer_Security_Update_for_Multiple_Issues

Vendor	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1519, CVE-2025-66418, CVE-2026-6474, CVE-2026-6637)
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	BIG-IP Next CNF - Versions 2.0.0 - 2.2.1 BIG-IP Next for Kubernetes Versions: • 2.3.0 • 2.0.0 - 2.2.1 BIG-IP (DNS) - Versions 21.0.0 BIG-IP Next SPK Versions: • 1.7.0 - 1.7.16 • 1.8.0 - 1.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000162286 • https://my.f5.com/manage/s/article/K000162114 • https://my.f5.com/manage/s/article/K000162479 • https://my.f5.com/manage/s/article/K000162478

Vendor	**Cisco**
Severity	**High**
Affected Vulnerability	Static Credential Vulnerability (CVE-2026-20316)
Description	Cisco has released a security update addressing a vulnerability that exists in their product. **CVE-2026-20316:** This vulnerability is due to the presence of static user credentials for a low-privileged account. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and access sensitive data as the low-privileged user. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Cisco Secure FMC Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-23240, CVE-2026-31738, CVE-2026-43038, CVE-2026-46113, CVE-2026-46120, CVE-2026-46173, CVE-2026-46227, CVE-2026-52909, CVE-2026-52943, CVE-2026-53359, CVE-2026-53362, CVE-2026-53366)
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 High Performance Computing 12 SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Live Patching 15-SP7 SUSE Linux Enterprise Micro 5.3, 5.4 & 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/

Vendor	**Asus**
Severity	**High**
Affected Vulnerability	Race Condition Vulnerability (CVE-2026-16727)
Description	Asus has released a security update addressing a vulnerability that exists in their product. **CVE-2026-16727:** Concurrent Execution using Shared Resource with Improper Synchronization (“Race Condition”) in ASUS Armoury Crate allows a local user to execute arbitrary code with elevated privileges via a crafted file replacement. Asus advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Armoury Crate versions earlier than V6.5.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.asus.com/security-advisory

Vendor	**Samba**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-6949, CVE-2026-58216, CVE-2025-58218, CVE-2026-58221, CVE-2026-58222, CVE-2026-58224)
Description	Samba 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. Samba advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Samba AD DC versions 4.0.0 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.samba.org/samba/security/CVE-2026-6949.html • https://www.samba.org/samba/security/CVE-2026-58216.html • https://www.samba.org/samba/security/CVE-2026-58218.html • https://www.samba.org/samba/security/CVE-2026-58221.html • https://www.samba.org/samba/security/CVE-2026-58222.html • https://www.samba.org/samba/security/CVE-2026-58224.html

Vendor	**NodeJS**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-56846, CVE-2026-56848, CVE-2026-58043, CVE-2026-56850, CVE-2026-58040, CVE-2026-58041, CVE-2026-58042, CVE-2026-58045, CVE-2026-56847, CVE-2026-58039, CVE-2026-58044)
Description	NodeJS 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. NodeJS advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	NodeJS Versions: • 26.x • 24.x • 22.x Dependencies • undici (8.9.0, 7.29.0, 6.28.0) on 26.x, 24.x, 22.x • llhttp (9.4.3) on 26.x, 24.x, 22.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/july-2026-security-releases#update-28-july-2026-security-releases-postponed

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8286, CVE-2026-8458, CVE-2026-8932, CVE-2026-9547, CVE-2026-16184, CVE-2026-14981, CVE-2026-15064, CVE-2026-15328, CVE-2026-15325, CVE-2026-14974, CVE-2026-14515, CVE-2026-16192, CVE-2026-14528, CVE-2026-14980, CVE-2026-2482, CVE-2026-14976, CVE-2026-15280)
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	AIX - Versions 7.3 IBM WebSphere Application Server - Versions 8.5 & 9.0 IBM WebSphere Application Server Liberty Versions 17.0.0.3 - 26.0.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7281628 • https://www.ibm.com/support/pages/node/7281625 • https://www.ibm.com/support/pages/node/7281631 • https://www.ibm.com/support/pages/node/7281721 • https://www.ibm.com/support/pages/node/7281641 • https://www.ibm.com/support/pages/node/7281648 • https://www.ibm.com/support/pages/node/7281649 • https://www.ibm.com/support/pages/node/7281651 • https://www.ibm.com/support/pages/node/7281633 • https://www.ibm.com/support/pages/node/7281743

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	18.04, 20.04, 22.04, 24.04, 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8547-2 • https://ubuntu.com/security/notices/USN-8615-1 • https://ubuntu.com/security/notices/USN-8616-1 • https://ubuntu.com/security/notices/USN-8617-1 • https://ubuntu.com/security/notices/USN-8618-1 • https://ubuntu.com/security/notices/USN-8570-2 • https://ubuntu.com/security/notices/USN-8574-3 • https://ubuntu.com/security/notices/USN-8595-3 • https://ubuntu.com/security/notices/USN-8619-1 • https://ubuntu.com/security/notices/USN-8620-1 • https://ubuntu.com/security/notices/USN-8615-2 • https://ubuntu.com/security/notices/USN-8620-2 • https://ubuntu.com/security/notices/USN-8622-1 • https://ubuntu.com/security/notices/USN-8623-1

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access Bypass Vulnerability (CVE-2026-18259)
Description	Drupal has released a security update addressing a vulnerability that exists in their product. **CVE-2026-18259:** The module does not sufficiently protect access token comparison in some cases. This could allow a persistent attacker to use a timing attack to guess a valid access token and bypass access restrictions for content protected by this module. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Token Content Access module - Versions prior to 3.1.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-090

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.