Advisory Alert

Alert Number: AAA20260813 **Date:** August 13, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
MongoDB	**Critical**	Improper Authentication Vulnerability
SUSE	**High**	Multiple Vulnerabilities
WordPress	**High**	Remote Code Execution Vulnerability
IBM	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Palo Alto Networks	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortinet	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Multiple Vulnerabilities
NETGEAR	**Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**MongoDB**
Severity	**Critical**
Affected Vulnerability	Improper Authentication Vulnerability (CVE-2026-18691)
Description	MongoDB has released a security update addressing a vulnerability that exists in their products. **CVE-2026-18691:** An issue in MongoDB Server's intra-cluster connection setup could allow a party with suitable network access to influence which authentication mechanism is used when one replica set member connects to another. Under certain conditions, this could cause the cluster's shared internal credential to be transmitted in a less-protected form, potentially allowing that credential to be recovered. If recovered, the credential could be used to authenticate as the internal superuser to nodes in the deployment. MongoDB advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	MongoDB Server versions: • prior to 8.3.8 • prior to 8.0.29 • prior to 7.0.40
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://jira.mongodb.org/browse/SERVER-130264

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
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 SUSE Linux Enterprise High Availability Extension 15 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4 and 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4, SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Real Time 15 SP4 and 15 SP5 SUSE Linux Enterprise Server 12 SP5, LTSS and LTSS Extended Securrity SUSE Linux Enterprise Server 15 SP4 and LTSS SUSE Linux Enterprise Server 15 SP5 and LTSS SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4 and 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE 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-20263595-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263594-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263593-1/

Vendor	**WordPress**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-65640)
Description	WordPress has released a security update addressing a vulnerability that exists in their products. **CVE-2026-65640:** Certain installations of WordPress are vulnerable to a remote code execution vulnerability via malicious Postscript file upload by an Author level user or higher. WordPress advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WordPress versions: • 7.0.0 - 7.0.3 • 6.9.0 - 6.9.6 • 6.8.0 - 6.8.7 • 6.7.0 - 6.7.6 • 6.6.0 - 6.6.6 • 6.5.0 - 6.5.9 • 6.4.0 - 6.4.9 • 6.3.0 - 6.3.9 • 6.2.0 - 6.2.10 • 6.1.0 - 6.1.11 • 6.0.0 - 6.0.13 • 5.9.0 - 5.9.15 • 5.8.0 - 5.8.14 • 5.7.0 - 5.7.16 • 5.6.0 - 5.6.18 • 5.5.0 - 5.5.19 • 5.4.0 - 5.4.20 • 5.3.0 - 5.3.22 • 5.2.0 - 5.2.25 • 5.1.0 - 5.1.23 • 5.0.0 - 5.0.26 • 4.9.0 - 4.9.30 • 4.8.0 - 4.8.29 • 4.7.0 - 4.7.34
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/08/wordpress-7-0-4-release/

Vendor	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-5588, CVE-2025-14813, CVE-2026-5598)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-5588**: Use of a Broken or Risky Cryptographic Algorithm vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcpkix on all (pkix modules), Legion of the Bouncy Castle Inc. BCPKIX-FIPS bcpkix on All (pkix modules), Legion of the Bouncy Castle Inc. BCPIX-LTS bcpkix on All (pkix modules). This vulnerability is associated with program files JcaContentVerifierProviderBuilder.Java, JcaContentVerfierProviderBuilder.Java. **CVE-2025-14813**: Use of a Broken or Risky Cryptographic Algorithm vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA bcprov on all (core modules). This vulnerability is associated with program files G3413CTRBlockCipher. **CVE-2026-5598**: Covert timing channel vulnerability in Legion of the Bouncy Castle Inc. BC-JAVA core on all (core modules). This vulnerability is associated with program files FrodoEngine.Java. IBM advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM DB2 Server versions 11.5.0 to 11.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7277422

Vendor	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53202, CVE-2026-53264, CVE-2026-63887, CVE-2026-64300, CVE-2026-45991, CVE-2026-53009, CVE-2025-54518, CVE-2026-43112)
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 Red Hat Enterprise Linux for x86_64 - Extended Update Support Red Hat Enterprise Linux for x86_64 - 4 years of updates Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions Red Hat Enterprise Linux Server - AUS Red Hat Enterprise Linux for IBM z Systems Red Hat Enterprise Linux for IBM z Systems - Extended Update Support Red Hat Enterprise Linux for IBM z Systems - 4 years of updates Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle Red Hat Enterprise Linux for Power, little endian Red Hat Enterprise Linux for Power, little endian - Extended Update Support Red Hat Enterprise Linux for Power, little endian - 4 years of support Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions Red Hat Enterprise Linux for ARM 64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support Red Hat Enterprise Linux for ARM 64 - 4 years of updates Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle Red Hat CodeReady Linux Builder for x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support Red Hat CodeReady Linux Builder for IBM z Systems Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support Red Hat CodeReady Linux Builder for Power, little endian Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support Red Hat CodeReady Linux Builder for ARM 64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:54343 https://access.redhat.com/errata/RHSA-2026:54246 https://access.redhat.com/errata/RHSA-2026:53990 https://access.redhat.com/errata/RHSA-2026:54443

Vendor	**Ubuntu**
Severity	**High**, **Medium**
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	Ubuntu 26.04, 24.04, 22.04, 20.4, 18.04, and 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8636-1 https://ubuntu.com/security/notices/USN-8635-1 https://ubuntu.com/security/notices/USN-8634-1 https://ubuntu.com/security/notices/USN-8633-1 https://ubuntu.com/security/notices/USN-8631-1 https://ubuntu.com/security/notices/USN-8630-1 https://ubuntu.com/security/notices/USN-8629-1

Vendor	**MongoDB**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-18703, CVE-2026-18707, CVE-2026-18706, CVE-2026-18687, CVE-2026-18695, CVE-2026-18688, CVE-2026-18692, CVE-2026-18704, CVE-2026-18705, CVE-2026-18693, CVE-2026-18697, CVE-2026-18701, CVE-2026-18700, CVE-2026-18696, CVE-2026-18708, CVE-2026-18694, CVE-2026-18702, CVE-2026-18699, CVE-2026-18690, CVE-2026-18698, CVE-2026-18709, CVE-2026-18711, CVE-2026-18712, CVE-2026-18710)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Server versions: prior to 8.3.8 prior to 8.0.29 prior to 7.0.40 MongoDB Driver versions: prior to 5.9.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**Palo Alto Networks**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-0301, CVE-2026-0299, CVE-2026-0297, CVE-2026-0296, CVE-2026-0295)
Description	Palo Alto Networks 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. Palo Alto Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PAN-OS 11.1 prior to: • 11.1.16-h1 • 11.1.17 PAN-OS 10.2 prior to 10.2.8 Prisma Access 10.2 prior to 10.2.10 GlobalProtect App 6.3: • prior to 6.3.3-h15 on Linux • prior to 6.3.3-h14 (6.3.3-1121) on macOS • prior 6.3.3-h14 (6.3.3-1121) on Windows • prior to 6.3.5 on iOS • prior to 6.3.5 on Android • prior to 6.3.5 on Chrome OS GlobalProtect App 6.2: • All on Linux • prior to 6.2.8-h13 (6.2.8-1045) on macOS • prior to 6.2.8-h13 (6.2.8-1045) on Windows GlobalProtect App 6.0: • prior to 6.0.15 on Linux • prior to 6.0.15 on macOS • prior to 6.0.15 on Windows • prior to 6.0.15 on iOS • prior to 6.0.15 on Android • prior to 6.0.15 on Chrome OS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-0301 https://security.paloaltonetworks.com/CVE-2026-0299 https://security.paloaltonetworks.com/CVE-2026-0298 https://security.paloaltonetworks.com/CVE-2026-0297 https://security.paloaltonetworks.com/CVE-2026-0296 https://security.paloaltonetworks.com/CVE-2026-0295

Vendor	**Fortinet**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-26035, CVE-2026-70466, CVE-2026-70468, CVE-2026-49975, CVE-2026-70465, CVE-2026-70467, CVE-2026-71407, CVE-2026-71408)
Description	Fortinet 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. Fortinet advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	FortiWeb 8.0 versions 8.0.0 through 8.0.2 FortiWeb 7.6 versions 7.6.0 through 7.6.5 FortiWeb 7.4 all versions FortiWeb 7.2 all versions FortiManager 7.6 version 7.6.1 FortiManager 7.4 versions 7.4.3 through 7.4.5 FortiManager 7.2 versions 7.2.5 through 7.2.9 FortiManager Cloud 7.6 version 7.6.1 FortiManager Cloud 7.4 versions 7.4.3 through 7.4.5 FortiManager Cloud 7.2 versions 7.2.5 through 7.2.9 FortiPAM 1.9 versions 1.9.0 through 1.9.1 FortiPAM 1.8, 1.7, 1.6, 1.5, 1.4, 1.3, 1.2, 1.1 and 1.0 - all versions FortiProxy 7.6 versions 7.6.0 through 7.6.6 FortiProxy 7.4 versions 7.4.0 through 7.4.14 FortiProxy 7.2 all versions FortiSwitchManager 7.2 versions 7.2.0 through 7.2.9 FortiClientWindows 7.4 versions 7.4.0 through 7.4.3 FortiClientWindows 7.2 versions 7.2.0 through 7.2.11 FortiSIEM 7.5 version 7.5.0 FortiSIEM 7.4 versions 7.4.0 through 7.4.2 FortiSIEM 7.3 versions 7.3.0 through 7.3.5 FortiSIEM 7.2, 7.1, 7.0, 6.7, 6.6, and 6.5 - all versions FortiOS 7.6 versions 7.6.0 through 7.6.6 FortiOS 7.4 and 7.2 - all versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-26-158 https://www.fortiguard.com/psirt/FG-IR-26-157 https://www.fortiguard.com/psirt/FG-IR-26-160 https://www.fortiguard.com/psirt/FG-IR-26-163 https://www.fortiguard.com/psirt/FG-IR-26-156 https://www.fortiguard.com/psirt/FG-IR-26-159 https://www.fortiguard.com/psirt/FG-IR-26-161 https://www.fortiguard.com/psirt/FG-IR-26-162

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-73476, CVE-2026-73475)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-73476:** The module does not sufficiently ensure exact matching of externally supplied identity values when storing and looking up authentication mappings under certain database collation configurations. **CVE-2026-73475:** The module doesn't sufficiently validate the transaction result in certain circumstances, allowing a malicious user to mark transactions placed without payment. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	External Authentication module versions prior to 2.0.13 Commerce PayPal module versions prior to 1.12.0 and 2.0.0 prior to 2.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-098 https://www.drupal.org/sa-contrib-2026-095

Vendor	**NETGEAR**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-11814, CVE-2026-11739, CVE-2026-11737, CVE-2026-11738, CVE-2026-9214, CVE-2026-11735, CVE-2026-11736, CVE-2026-11733, CVE-2026-11734)
Description	NETGEAR 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. NETGEAR 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://kb.netgear.com/000070887/August-2026-NETGEAR-Security-Advisory

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 threat