Advisory Alert

Alert Number: AAA20260828 **Date:** August 28, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
WatchGuard	**Critical**	Multiple Vulnerabilities
Veeam	**Critical**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SolarWinds	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
WatchGuard	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities
Ubuntu	**High**, Medium, Low	Multiple Vulnerabilities
Veeam	**Medium**	Security Update
Drupal	**Medium**	Multiple Vulnerabilities
Dell	**Medium**	Improper Access Control Vulnerability
F5	**Medium**	Security Update
cPanel	**Medium**, Low	Multiple Vulnerabilities
OpenSSL	**Medium**, Low	Multiple Vulnerabilities

Description

Vendor	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-57909, CVE-2026-57910, CVE-2026-19313, CVE-2026-19318, CVE-2026-13086, CVE-2026-19315, CVE-2026-78174)
Description	WatchGuard 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. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	WatchGuard Agent versions prior to 1.25.13.0000 Fireware OS versions: • Default - >= 2025.0, < 2026.2.2, >= 12.0, < 12.12.2 • T15/T35 - >= 12.0, < 12.5.20 Dimension versions: • >= 2.0 • < 2.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-57909/ https://psirt.watchguard.com/CVE-2026-57910/ https://psirt.watchguard.com/CVE-2026-19313/ https://psirt.watchguard.com/CVE-2026-19318/ https://psirt.watchguard.com/CVE-2026-13086/ https://psirt.watchguard.com/CVE-2026-19315/ https://psirt.watchguard.com/CVE-2026-78174/

Vendor	**Veeam**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-65641)
Description	Veeam has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-65641:** A vulnerability allowing an unauthenticated network attacker to coerce SMB authentication from the service account. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam ONE 13.1.0.7034 and all earlier version 13 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4905

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29371, CVE-2025-14813, CVE-2025-67030, CVE-2026-0636, CVE-2026-1605, CVE-2026-2332, CVE-2026-3505, CVE-2026-40542, CVE-2026-41409, CVE-2026-41635, CVE-2026-42778, CVE-2026-42779, CVE-2026-47065, CVE-2026-50193, CVE-2026-53435, CVE-2026-53437, CVE-2026-54399, CVE-2026-54428, CVE-2026-54512, CVE-2026-5588, CVE-2026-56624, CVE-2026-57280, CVE-2026-57281, CVE-2026-68494, CVE-2026-70426, CVE-2026-70427, CVE-2026-70428, CVE-2026-70429, CVE-2025-68121, CVE-2026-25679, CVE-2026-32280, CVE-2026-33811, CVE-2026-42499, CVE-2026-74581, CVE-2026-52924, CVE-2026-63886, CVE-2026-63913, CVE-2026-64189, CVE-2026-64191, CVE-2026-64276, CVE-2026-64277, CVE-2026-64320, CVE-2025-68211, CVE-2026-23003, CVE-2026-43114, CVE-2026-52920, CVE-2026-53131, CVE-2026-53185, CVE-2026-53268, CVE-2025-54518, CVE-2026-3833, CVE-2026-29111, CVE-2026-33845, CVE-2026-33846, CVE-2026-34982, CVE-2026-35177, CVE-2026-41411, CVE-2026-43112, CVE-2026-46483, CVE-2026-48864, CVE-2026-1933, CVE-2026-2340, CVE-2026-3012, CVE-2026-4408, CVE-2026-5260, CVE-2026-5450, CVE-2026-14474, CVE-2026-14476, CVE-2026-42009, CVE-2026-42010, CVE-2026-42011, CVE-2026-42013, CVE-2026-64531, CVE-2026-32283, CVE-2026-39820, CVE-2026-27145, CVE-2026-42504)
Description	Red Hat 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. Red Hat 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://access.redhat.com/security/security-updates/

Vendor	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-66152, CVE-2026-66153)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-66152:** A Path traversal vulnerability in OPSWAT tarball in the SonicWall NetExtender Linux client allows an attacker to write arbitrary file as root. **CVE-2026-66153:** The NEService auto-upgrade process insecurely handles temporary files in SonicWall NetExtender Linux client which allows an attacker to manipulate file paths. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetExtender Linux Client Version 10.3.5 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0013

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 and 15.6 • SUSE Linux Enterprise Server 11 SP4 • SUSE Linux Enterprise Server 11 SP4 LTSS EXTREME CORE • SUSE Linux Enterprise Server 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP4 and 15 SP5 • SUSE Linux Enterprise Live Patching 12-SP5, 15-SP4, 15-SP5, 15-SP6 and 15-SP7 • SUSE Linux Enterprise Real Time 15 SP4, 15 SP5, 15 SP6 and 15 SP7 • SUSE Linux Enterprise Micro 5.3, 5.4 and 5.5 • SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20263829-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263826-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263821-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263820-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263819-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263810-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263809-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263808-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20263807-1/

Vendor	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-81851, CVE-2026-78008, CVE-2026-19316, CVE-2026-78009, CVE-2026-78010, CVE-2026-19317, CVE-2026-19314, CVE-2026-78011, CVE-2026-78614, CVE-2026-13108, CVE-2026-78500, CVE-2026-78618, CVE-2026-78499, CVE-2026-78610, CVE-2026-78047, CVE-2026-78617, CVE-2026-78495, CVE-2026-78613, CVE-2026-78103, CVE-2026-78615, CVE-2026-78612, CVE-2026-78195, CVE-2026-78498, CVE-2026-78616)
Description	WatchGuard 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. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS Versions: • Default - >= 2025.0, < 2026.2.2, >= 12.0, < 12.12.2 • T15/T35 - >= 12.0, < 12.5.20 • EUCC - >= 12.0, < 12.11.9 Dimension Versions • >= 2.0 • < 2.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-48779, CVE-2026-11525, CVE-2026-12151, CVE-2026-6733, CVE-2026-6734, CVE-2026-9678, CVE-2026-9679, CVE-2026-9697, CVE-2026-13149, CVE-2026-45822, CVE-2026-5038, CVE-2026-5079, CVE-2026-8723, CVE-2026-12143, CVE-2026-53550, CVE-2026-59887, CVE-2026-59724, CVE-2026-59725, CVE-2026-59869, CVE-2026-44486, CVE-2026-44487, CVE-2026-44488, CVE-2026-44489, CVE-2026-44490, CVE-2026-44492, CVE-2026-44494, CVE-2026-44496, CVE-2026-46625, CVE-2026-53537, CVE-2026-53538, CVE-2026-53539, CVE-2026-53540, CVE-2026-59890, CVE-2026-45149, CVE-2026-40895, CVE-2026-45736, CVE-2026-62389, CVE-2026-5078, CVE-2026-48801, CVE-2026-34481, CVE-2026-69247, CVE-2026-69248, CVE-2026-69249)
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	QRadar AI Assistant 1.0.0 to 2.1.1 IBM Security QRadar EDR 3.12 to 3.12.25
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7285376 https://www.ibm.com/support/pages/node/7285380

Vendor	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53309, CVE-2026-53246, CVE-2026-53224, CVE-2026-53043, CVE-2026-52993, CVE-2026-52914, CVE-2026-43071, CVE-2026-53359, CVE-2026-53228, CVE-2026-53212, CVE-2026-53176, CVE-2026-53088, CVE-2026-53045, CVE-2026-53006, CVE-2026-53002, CVE-2026-52999, CVE-2026-52989, CVE-2026-52986, CVE-2026-52982, CVE-2026-52958, CVE-2026-52955, CVE-2026-52931, CVE-2026-52924, CVE-2026-46331, CVE-2026-46266, CVE-2026-43499, CVE-2026-43493, CVE-2026-43198, CVE-2026-31668, CVE-2026-31657, CVE-2026-31448, CVE-2026-31414, CVE-2026-31405, CVE-2026-23392, CVE-2025-27558, CVE-2021-47378, CVE-2026-64531, CVE-2026-53247, CVE-2026-53225, CVE-2026-53215, CVE-2026-53151, CVE-2026-46325, CVE-2026-46242, CVE-2026-43465, CVE-2026-43197, CVE-2026-53086, CVE-2026-43378, CVE-2026-31705)
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 14.04, 16.04, 18.04, 20.04, 22.04, 24.04 and 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8661-3 https://ubuntu.com/security/notices/USN-8658-4 https://ubuntu.com/security/notices/USN-8643-5 https://ubuntu.com/security/notices/USN-8659-4 https://ubuntu.com/security/notices/USN-8666-2 https://ubuntu.com/security/notices/USN-8630-5 https://ubuntu.com/security/notices/USN-8658-3 https://ubuntu.com/security/notices/USN-8643-4 https://ubuntu.com/security/notices/USN-8659-3 https://ubuntu.com/security/notices/USN-8666-3 https://ubuntu.com/security/notices/USN-8644-3

Vendor	**Veeam**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2026-58070)
Description	Veeam has released a security update addressing a vulnerability that exists in their products. **CVE-2026-58070:** A vulnerability that causes guest OS credentials used for Application Aware processing to be recorded in cleartext in logs on the guest machine. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 13.0.2.29 and all earlier version 13 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4902

Vendor	**Drupal**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-81158, CVE-2026-81269, CVE-2026-81205, CVE-2026-18260)
Description	Drupal 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. Drupal advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Entity API module versions prior to 1.8.0 Data field module versions prior to 2.0.13 Disable Login Page module versions prior to 1.1.4 LDAP / Active Directory Integration module versions prior to 2.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2026-113 https://www.drupal.org/sa-contrib-2026-108 https://www.drupal.org/sa-contrib-2026-111 https://www.drupal.org/sa-contrib-2026-115 https://www.drupal.org/sa-contrib-2026-110

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Improper Access Control Vulnerability (CVE-2026-79940)
Description	Dell has released a security update addressing a vulnerability that exists in their products. **CVE-2026-79940:** Dell iDRAC9, 14G versions prior to 7.00.00.182 and 15G/16G versions prior to 7.20.30.50, contains an Improper Access Control vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to gaining access to unauthorized data. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC9 Versions prior to: 7.20.30.50 7.00.00.182
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000502514/dsa-2026-374-security-update-for-dell-idrac9-vulnerability

Vendor	**F5**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-15281)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2025-15281:** Calling wordexp with WRDE_REUSE in conjunction with WRDE_APPEND in the GNU C Library version 2.0 to version 2.42 may cause the interface to return uninitialized memory in the we_wordv member, which on subsequent calls to wordfree may abort the process. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next for Kubernetes version 2.2.0 and 2.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000163028

Vendor	**cPanel**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-66299, CVE-2026-26962)
Description	cPanel has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-66299:** Denial of service in the WebSocket chat example. **CVE-2026-26962:** Improper unfolding of folded multipart headers preserves CRLF in parsed parameter values. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-tomcat101 version v10.1.57 ea-ruby27-rubygem-rack version v2.2.23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

Vendor	**OpenSSL**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-75803, CVE-2026-14457, CVE-2026-18798, CVE-2026-54874, CVE-2026-63072, CVE-2026-63073, CVE-2026-63074, CVE-2026-63075, CVE-2026-63076)
Description	OpenSSL 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. OpenSSL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSSL versions: • from 4.0.0 before 4.0.2 • from 3.6.0 before 3.6.4 • from 3.5.0 before 3.5.8 • from 3.4.0 before 3.4.7 • from 3.0.0 before 3.0.22 • from 1.1.1 before 1.1.1zi • from 1.0.2 before 1.0.2zr
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/

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.