Advisory Alert

Alert Number: AAA20260923 **Date:** September 23, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
SolarWinds	**Critical**	Remote Code Execution Vulnerability
WordPress	**Critical**	Remote File Inclusion Vulnerability
F5	**Critical**	Remote Code Execution Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
CheckPoint	**High**	Directory Traversal and File Upload Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SolarWinds	**High**	Remote Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-28324)
Description	SolarWinds has released a security update addressing a vulnerability that exists in their products. **CVE-2026-28324:** SolarWinds Observability Self-Hosted was found to be affected by an unauthenticated remote code execution vulnerability due to the insufficient integrity checks. Installations configured in a non-default and non-secure configuration are affected. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Observability Self-Hosted 2026.2.2 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28324

Vendor	**WordPress**
Severity	**Critical**
Affected Vulnerability	Remote File Inclusion Vulnerability (CVE-2026-87902)
Description	WordPress has released a security update addressing a vulnerability that exists in their products. **CVE-2026-87902**: An unauthenticated attacker can make get_page_template() page-template resolution include a chosen readable local .php file outside the active theme directories. If relevant pre-conditions for both the server environment and the active theme are met, this can lead to RCE. WordPress advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	WordPress versions: • 7.1.0 - 7.1.1 • 7.0.0 - 7.0.5 • 6.9.0 - 6.9.8 • 6.8.0 - 6.8.9 • 6.7.0 - 6.7.8 • 6.6.0 - 6.6.8 • 6.5.0 - 6.5.11 • 6.4.0 - 6.4.11 • 6.3.0 - 6.3.11 • 6.2.0 - 6.2.12 • 6.1.0 - 6.1.13 • 6.0.0 - 6.0.15 • 5.9.0 - 5.9.17 • 5.8.0 - 5.8.16 • 5.7.0 - 5.7.18 • 5.6.0 - 5.6.20 • 5.5.0 - 5.5.21 • 5.4.0 - 5.4.22 • 5.3.0 - 5.3.24 • 5.2.0 - 5.2.27 • 5.1.0 - 5.1.25 • 5.0.0 - 5.0.28 • 4.9.0 - 4.9.32 • 4.8.0 - 4.8.31 • 4.7.0 - 4.7.36
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wordpress.org/news/2026/09/wordpress-7-1-2-release/

Vendor	**F5**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-94127)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-94127:** When a BIG-IP APM access policy and an OAuth profile are configured on a virtual server, specific malicious traffic can lead to remote code execution (RCE). This vulnerability is only present when BIG-IP APM is configured as an OAuth Authorization Server. Deployments using APM strictly as an OAuth Client / Resource Server (without OAuth authorization server profiles configured) are not affected by this vulnerability. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP APM verions: • 21.1.0 • 17.5.0 - 17.5.1 and 17.1.0 - 17.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000162605

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-14525, CVE-2026-14529)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-14525:** IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 IBM WebSphere Application Server Liberty is vulnerable to an authentication bypass when the rtcomm-1.0 or rtcommGateway-1.0 feature is enabled. **CVE-2026-14529:** IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 traditional is vulnerable to server-side request forgery (SSRF) when the SIP container feature (sipServlet-1.1) is enabled. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerVM Novalink versions: • 2.2.0 • 2.2.1 • 2.2.1.1 • 2.3.0 • 2.3.0.1 • 2.3.1 • 2.3.2 • 2.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288949

Vendor	**CheckPoint**
Severity	**High**
Affected Vulnerability	Directory Traversal and File Upload Vulnerability (CVE-2026-93616)
Description	CheckPoint has released a security update addressing a vulnerability that exists in their products. **CVE-2026-93616:** A directory traversal and file upload vulnerability allows an unauthenticated attacker to upload and execute arbitrary scripts on the Check Point Management Server. This vulnerability is exploited in the Wild. Check Point is aware of a handful of customers who have been attacked. CheckPoint advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	R82.20 R82.10 Jumbo Hotfix Take 44 or lower R82 Jumbo Hotfix Take 126 or lower R81.20 Jumbo Hotfix Take 166 or lower R81.10 Jumbo Hotfix Take 190 or lower (EoS) R80, R80.10, R80.20, R80.30, R80.40, R81 (all EoS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk1000171/

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-39964, CVE-2026-45894, CVE-2026-45959, CVE-2026-53062, CVE-2026-63823, CVE-2026-64534, CVE-2026-68155, CVE-2026-68159, CVE-2026-68188, CVE-2026-68293, CVE-2026-68391, CVE-2026-74518, CVE-2025-21826, CVE-2026-64017, CVE-2026-64368, CVE-2026-64564, CVE-2026-24281, CVE-2026-24308, CVE-2026-33871, CVE-2026-46150, CVE-2026-53196, CVE-2026-64191, CVE-2026-3505, CVE-2026-5680, CVE-2026-10832, CVE-2026-14180, CVE-2026-15554, CVE-2026-15555, CVE-2026-15560, CVE-2026-15561, CVE-2026-15562, CVE-2026-15563, CVE-2026-15565, CVE-2026-15567, CVE-2026-44417, CVE-2026-46581, CVE-2026-49362, CVE-2026-49363, CVE-2026-49364, CVE-2026-49875, CVE-2026-50632, CVE-2026-54512, CVE-2026-54513, CVE-2026-54515, CVE-2026-55831, CVE-2026-55833, CVE-2026-56745, CVE-2026-56746, CVE-2026-57967, CVE-2026-59649, CVE-2026-59889, CVE-2026-59899, CVE-2026-62243, CVE-2026-68494, CVE-2026-69152, CVE-2026-73508, CVE-2026-85511, CVE-2026-86404, CVE-2023-53781, CVE-2026-52993, CVE-2026-53002, CVE-2026-64268, CVE-2026-63887, CVE-2026-63888, CVE-2026-31692, CVE-2026-53185)
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 7 Extended Life Cycle Support: • s390x • ppc64 • ppc64le • x86_64 Red Hat Enterprise Linux 8: • AUS: 8.4, 8.6 (x86_64) • Extended Life Cycle Long Life: 8.4, 8.6, 8.8 (aarch64, ppc64le, s390x, x86_64) • TUS: 8.8 (x86_64) • Update Services for SAP Solutions: 8.8 (ppc64le, x86_64) Red Hat Enterprise Linux 9: 4 Years of Updates: 9.4, 9.6 (aarch64, s390x) AUS: 9.4, 9.6 (x86_64) • CodeReady Linux Builder - Extended Update Support: 9.6 (aarch64, ppc64le, s390x, x86_64) • Extended Life Cycle: 9.4, 9.6 (aarch64, ppc64le, s390x, x86_64) • Extended Update Support: 9.6 (aarch64, ppc64le, s390x, x86_64) • Update Services for SAP Solutions: 9.4, 9.6 (ppc64le, x86_64) Red Hat Enterprise Linux 10 Base & CodeReady Builder: • Base: 10 (aarch64, ppc64le, s390x, x86_64) • CodeReady Linux Builder: 10 (aarch64, ppc64le, s390x, x86_64) Red Hat Enterprise Linux 10.2: • 4 Years of Support / Updates (aarch64, ppc64le, s390x, x86_64) • CodeReady Linux Builder - Extended Update Support (aarch64, ppc64le, s390x, x86_64) • Extended Life Cycle (aarch64, ppc64le, s390x, x86_64) • Extended Update Support (aarch64, ppc64le, s390x, x86_64) JBoss Enterprise Application Platform: • JBoss EAP Text-Only Advisories (x86_64) • JBoss EAP 8.1 for RHEL 10 (x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:70498 https://access.redhat.com/errata/RHSA-2026:70484 https://access.redhat.com/errata/RHSA-2026:70421 https://access.redhat.com/errata/RHSA-2026:70290 https://access.redhat.com/errata/RHSA-2026:70277 https://access.redhat.com/errata/RHSA-2026:70230 https://access.redhat.com/errata/RHSA-2026:69908 https://access.redhat.com/errata/RHSA-2026:69906 https://access.redhat.com/errata/RHSA-2026:69874 https://access.redhat.com/errata/RHSA-2026:69837

Vendor	**SolarWinds**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-28325)
Description	SolarWinds has released a security update addressing a vulnerability that exists in their products. **CVE-2026-28325:** SolarWinds Observability Self-Hosted was found to be affected by an unauthenticated remote code execution vulnerability stemming from deserialization of untrusted data when the application is configured to use a specific communication mode. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Observability Self-Hosted 2026.2.2 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28325

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	SUSE Linux Enterprise 12 SP5: • High Performance Computing • Live Patching • Server • Server LTSS & Extended Security • Server for SAP Applications SUSE Linux Enterprise 15 SP4: • High Availability Extension • High Performance Computing (Base, ESPOS, LTSS) • Live Patching • Real Time • Server (Base, LTSS) • Server for SAP Applications SUSE Linux Enterprise Micro: • 5.3 (Base, for Rancher) • 5.4 (Base, for Rancher) SUSE Manager 4.3: • Proxy • Retail Branch Server • Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264282-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264279-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264284-1/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-61308, CVE-2026-70907, CVE-2026-60589, CVE-2026-16440, CVE-2026-10571, CVE-2026-18499, CVE-2026-10841, CVE-2026-11548, CVE-2026-11549, CVE-2026-11722, CVE-2026-15396, CVE-2026-15412, CVE-2026-15634, CVE-2026-57819, CVE-2026-54225, CVE-2026-64958, CVE-2026-14980, CVE-2026-2482, CVE-2026-16192, 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	PowerVM Novalink versions: • 2.1.1 • 2.2.0 • 2.2.1 • 2.2.1.1 • 2.3.0 • 2.3.0.1 • 2.3.1 • 2.3.2 • 2.3.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288865 https://www.ibm.com/support/pages/node/7288949

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	Ubuntu 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-8802-1 https://ubuntu.com/security/notices/USN-8728-2 https://ubuntu.com/security/notices/USN-8726-4 https://ubuntu.com/security/notices/USN-8729-4 https://ubuntu.com/security/notices/USN-8730-5 https://ubuntu.com/security/notices/USN-8793-2

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.