Advisory Alert

Alert Number: AAA20261022 **Date:** October 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
SolarWinds	**Critical**	Unauthenticated Remote Code Execution Vulnerabilities
cPanel	**Critical**	Unauthenticated Remote Code Execution Vulnerabilities
PHP	**Critical**	Unauthenticated Remote Code Execution Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Palo Alto Networks	**High**	Unauthenticated Remote Code Execution Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
SolarWinds	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
NetApp	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NodeJS	**High**, **Medium**, **Low**	Multiple Vulnerabilities
cPanel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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 OpenShift AI
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:87410 https://access.redhat.com/errata/RHSA-2026:86891

Vendor	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	SolarWinds has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Pingdom and SolarWinds External Websites
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-109618-and-cve-2026-109619

Vendor	**cPanel**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	cPanel & WHM versions prior to 138.0.18, 136.0.50, 134.0.66 and 110.0.153 EasyApache: • ea-php74 • ea-php80 • ea-php81 • ea-php82 • ea-php83 • ea-php84 • ea-php85
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/138-change-log/#138018 https://docs.cpanel.net/changelogs/136-change-log/#136050 https://docs.cpanel.net/changelogs/134-change-log/#134066 https://docs.cpanel.net/changelogs/110-change-log/#1100153 https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2591

Vendor	**PHP**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	PHP has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). PHP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PHP Versions prior to 8.5.12, 8.4.27, 8.3.36 and 8.2.35
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/archive/2026.php#2026-10-21-5

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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	IBM Guardium External S-TAP version 12.2 IBM Guardium Data Protection versions 12.2.3, 12.2.4 and 12.1 AIX versions 7.3 and 7.2 VIOS version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293029 https://www.ibm.com/support/pages/node/7293412 https://www.ibm.com/support/pages/node/7293284 https://www.ibm.com/support/pages/node/7293282 https://www.ibm.com/support/pages/node/7293240 https://www.ibm.com/support/pages/node/7293412

Vendor	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76473, CVE-2026-76474, CVE-2026-76475, CVE-2026-76476, CVE-2026-76477, CVE-2026-76478, CVE-2026-76479, CVE-2026-76481, CVE-2026-76466, CVE-2026-20043, CVE-2026-20236, CVE-2026-20291, CVE-2026-20356)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-hardening-twgbH9e3 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vcs-static-cred-hr7EWZ8t • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-snort3-ybgmhTQe

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-64114, CVE-2026-64266, CVE-2026-64572, CVE-2026-68202, CVE-2026-80536, CVE-2026-80590, CVE-2026-89777, CVE-2026-99999, CVE-2026-91765, CVE-2026-109618, CVE-2026-109619, CVE-2025-1218, CVE-2025-14181, CVE-2026-6103, CVE-2026-91766, CVE-2026-91767, CVE-2026-91768, CVE-2026-91769, CVE-2026-92842, CVE-2026-93682, CVE-2026-68121)
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 Platform & Enterprise Software: • Red Hat OpenShift Container Platform 4.19 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat Enterprise Linux 8: • Base & CRB 8: aarch64, ppc64le, s390x, x86_64 • 8.6 & 8.8: Extended Life Cycle Long Life (x86_64), Advanced Update Support (AUS) (x86_64) • 8.8: Update Services (TUS) (x86_64), Update Services for SAP Solutions (ppc64le, x86_64) • 8.10: Extended Life Cycle (all archs) • Real Time & Real Time for NFV: x86_64 Red Hat Enterprise Linux 9: • Base & CRB 9: aarch64, ppc64le, s390x, x86_64 • 9.6: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), Extended Update Support (EUS) & CodeReady Linux Builder EUS (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64) • 9.8: Extended Life Cycle (all archs), Extended Update Support (EUS) & CodeReady Linux Builder EUS (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:87375 https://access.redhat.com/errata/RHSA-2026:87374 https://access.redhat.com/errata/RHSA-2026:87264 https://access.redhat.com/errata/RHSA-2026:87151 https://access.redhat.com/errata/RHSA-2026:87098 https://access.redhat.com/errata/RHSA-2026:87086 https://access.redhat.com/errata/RHSA-2026:87080 https://access.redhat.com/errata/RHSA-2026:87079 https://access.redhat.com/errata/RHSA-2026:87072 https://access.redhat.com/errata/RHSA-2026:83479

Vendor	**Palo Alto Networks**
Severity	**High**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	Palo Alto Networks has released a security update addressing a vulnerability that exists in their products. Palo Alto Networks advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	PAN-OS versions: • 12.2 All • 12.1 All • 11.2 All • 11.1 All • 10.2 All Panorama All Versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2026-109618

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53131, CVE-2026-63794, CVE-2026-63795, CVE-2026-63887, CVE-2026-68158, CVE-2026-109618, CVE-2026-109619)
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 12 SP5: High Performance Computing, Live Patching, Server, Server for SAP Applications • SUSE Linux Enterprise 15 SP4: High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications • SUSE Linux Enterprise 15 SP5: High Performance Computing, Live Patching, Real Time, Server, Server for SAP Applications • SUSE Linux Enterprise 15 SP6: Live Patching, Real Time, Server (including LTSS), Server for SAP Applications • SUSE Linux Enterprise 15 SP7: Server, Server for SAP Applications, Web and Scripting Module • SUSE Linux Enterprise Micro: 5.3, 5.4, 5.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264831-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264843-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264844-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264812-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264793-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264791-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264785-1/

Vendor	**SolarWinds**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-28328, CVE-2026-28331, CVE-2026-28330, CVE-2026-28329)
Description	SolarWinds 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. SolarWinds advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SolarWinds Observability Self-Hosted 2026.2.3 and below SolarWinds Patch Manager 2026.2 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28328 https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28331 https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28330 https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28329

Vendor	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76462, CVE-2026-76524, CVE-2026-76490, CVE-2026-76491, CVE-2026-76492, CVE-2026-76493, CVE-2026-76494, CVE-2026-76495, CVE-2026-76496, CVE-2026-76497, CVE-2026-76505, CVE-2026-20218, CVE-2026-20019, CVE-2026-20179, CVE-2026-20197, CVE-2026-76489, CVE-2026-20011, CVE-2026-76445, CVE-2026-20221, CVE-2026-76435, CVE-2026-76487)
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	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sec-client-priv-esc-muF8eZdm • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-opensrc-snort3-2fXGJPfe • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-exwy-hardening-FhcqBVcs • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr9k-tUyxcyXN • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-vba-bufdos-jAuFdvn9 • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-misc-dos-6mB22qAK • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-mime-vulns-bkXjcKkt • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-gtpcodec-dos-Rmecfepz • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-gre-JNpMHrTv • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-inf-disc-vvYqgSTS • https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-access-PW9e8Jt2

Vendor	**NetApp**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-13009, CVE-2026-50193, CVE-2026-32778)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-13009:** Successful exploitation of this vulnerability could lead to disclosure of sensitive information or addition or modification of data. **CVE-2026-50193:** FasterXML jackson-databind versions 2.10.0 prior to 2.14.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2026-32778:** libexpat versions prior to 2.7.5 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). NetApp advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• Active IQ Unified Manager: Microsoft Windows, VMware vSphere • NetApp HCI Baseboard Management Controller (BMC): H610S • ONTAP: 9 • Snap Center Plug-in for VMware vSphere • Snap Creator Framework
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261021-0002 https://security.netapp.com/advisory/ntap-20261021-0006 https://security.netapp.com/advisory/ntap-20261021-0018

Vendor	**NodeJS**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-106073, CVE-2026-106071, CVE-2026-106070, CVE-2026-106074, CVE-2026-106072, CVE-2026-105481, CVE-2026-111497, CVE-2026-106069, CVE-2026-105483, CVE-2026-105482)
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	Node.js versions 26.x, 24.x, and 22.x.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nodejs.org/en/blog/vulnerability/october-2026-security-releases

Vendor	**cPanel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-92392, CVE-2026-107929, CVE-2026-94266, CVE-2026-92391, CVE-2026-92390, CVE-2026-92389, CVE-2026-92388, CVE-2026-92387, CVE-2026-92386, CVE-2026-87865, CVE-2026-87863, CVE-2026-87862, CVE-2026-86414, CVE-2026-86410, CVE-2026-15176, CVE-2026-93479, CVE-2026-97205, CVE-2026-97629, CVE-2026-101025, CVE-2026-101019, CVE-2026-61812, CVE-2026-61813, CVE-2026-73856, CVE-2026-73857, CVE-2026-103932, CVE-2026-104259, CVE-2026-104269)
Description	cPanel 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. cPanel advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	EasyApache: • ea-libcurl • ea-nginx • ea-nginx-njs • ea-modsec30
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/#2591

Vendor	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-114531, CVE-2026-107260, CVE-2026-114532, CVE-2026-114533, CVE-2026-114534, CVE-2026-114535, CVE-2026-114536, CVE-2026-114537, CVE-2026-114538, CVE-2026-114539, CVE-2026-114543, CVE-2026-114541, CVE-2026-114553, CVE-2026-114542, CVE-2026-114544, CVE-2026-114545, CVE-2026-114546, CVE-2026-114548, CVE-2026-107256, CVE-2026-114572, CVE-2026-114555, CVE-2026-114554, CVE-2026-114571, CVE-2026-114573)
Description	Drupal 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. Drupal 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.drupal.org/security

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
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	IBM Guardium Data Protection versions 12.2.3, 12.2.4 and 12.1 IBM Guardium External S-TAP version 12.2 AIX versions 7.3 and 7.2 VIOS version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7293412 https://www.ibm.com/support/pages/node/7293240 https://www.ibm.com/support/pages/node/7293277 https://www.ibm.com/support/pages/node/7293282 https://www.ibm.com/support/pages/node/7293284 https://www.ibm.com/support/pages/node/7293412 https://www.ibm.com/support/pages/node/7293293 https://www.ibm.com/support/pages/node/7293294 https://www.ibm.com/support/pages/node/7293029

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.