Advisory Alert

Alert Number: AAA20261104 **Date:** November 4, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
NetApp	**Critical**	Authentication Bypass Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
SonicWall	**Critical**	Multiple Vulnerabilities
Citrix	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
SolarWinds	**Critical**	Command Injection Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
SolarWinds	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
NetApp	**Medium**	Authentication Bypass Vulnerability

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-95731, CVE-2026-95732, CVE-2026-95733)
Description	HPE has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-95731:** Hardcoded password vulnerabilities in the command-line interface of HPE Networking Fabric Composer could allow an unauthenticated remote attacker to access the affected system using hardcoded credentials. Successful exploitation could allow an attacker to gain unauthorized administrative access to the affected system with elevated privileges. **CVE-2026-95732:** A vulnerability exists in a component of HPE Networking Fabric Composer. Successful exploitation could allow an unauthenticated adjacent attacker to execute arbitrary code on the affected system. **CVE-2026-95733:** An authentication bypass vulnerability exists in the underlying operating system of HPE Networking Fabric Composer. Successful exploitation could allow an unauthenticated adjacent attacker to execute arbitrary code on the affected system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• HPE Networking Fabric Composer (AFC) 7.4.0 and below • HPE Networking Fabric Composer (AFC) 7.3.4 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05172en_us&docLocale=en_US

Vendor	**NetApp**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-22058)
Description	NetApp has released a security update addressing a vulnerability that exists in their products. **CVE-2026-22058:** StorageGRID (formerly StorageGRID Webscale) versions 11.3 and higher allow an attacker with product-specific knowledge and the ability to communicate with the Grid Network on certain ports to make unauthorized requests. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261103-0001

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-98432, CVE-2025-71066, CVE-2026-43051, CVE-2026-46259, CVE-2026-53062, CVE-2026-53073, CVE-2026-64007, CVE-2026-64534, CVE-2026-74556, CVE-2026-89481, CVE-2025-39797, CVE-2026-63974, CVE-2025-21702, CVE-2026-46086, CVE-2026-53224, CVE-2026-53246)
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	RHEL 8.4: • Extended Life Cycle Long Life (ELLL): x86_64 • Advanced Update Support (AUS): x86_64 RHEL 8.8: • Extended Life Cycle Long Life (ELLL): x86_64 • Telecommunications Update Service (TUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 RHEL 9.2: • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 RHEL 10.0: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • 4 Years of Updates/Support: aarch64, ppc64le, s390x, x86_64 RHEL 9.6: • Extended Update Support (EUS): aarch64, ppc64le, s390x, x86_64 • Advanced Update Support (AUS): x86_64 • Update Services for SAP Solutions: ppc64le, x86_64 • CodeReady Linux Builder EUS: aarch64, ppc64le, s390x, x86_64 • 4 Years of Updates: aarch64, s390x • Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:94623 • https://access.redhat.com/errata/RHSA-2026:94303 • https://access.redhat.com/errata/RHSA-2026:94477 • https://access.redhat.com/errata/RHSA-2026:94508 • https://access.redhat.com/errata/RHSA-2026:94438

Vendor	**SonicWall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109593, CVE-2026-109594)
Description	SonicWall has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109593:** An unauthenticated attacker with network access to the SonicWall GMS 9.5.2 and earlier versions may be able to read internal GMS files, potentially exposing sensitive information. **CVE-2026-109594:** Post-authentication Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability has been identified in the End-of-Life SonicWall GMS 9.5.2 and earlier versions which in specific conditions could potentially allow an authenticated attacker to access or modify information stored in the GMS database. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	GMS - Virtual Appliance and Windows Versions - 9.5.2 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0019

Vendor	**Citrix**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-98432, CVE-2026-102703, CVE-2026-97631, CVE-2026-45447, CVE-2024-38797, CVE-2024-38796, CVE-2022-36764, CVE-2022-36763)
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 8.4 and XenServer 9 • Workload Balancing (before 2026.1.1) • Conversion Manager (before 2026.2.0)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697256&articleURL=XenServer_Security_Update_for_Multiple_Issues

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-66909, CVE-2026-65583, CVE-2026-64564, CVE-2026-64534, CVE-2026-64102, CVE-2026-64034, CVE-2026-63994, CVE-2026-53049, CVE-2026-63687, CVE-2026-61466, CVE-2026-63992, CVE-2026-6653, CVE-2026-50252, CVE-2026-46043, CVE-2026-44172, CVE-2026-32327, CVE-2026-82717, CVE-2026-81642, CVE-2026-80714, CVE-2026-76183, CVE-2026-89972, CVE-2026-89846, CVE-2026-89530, CVE-2026-86248, CVE-2026-68159, CVE-2026-68156, CVE-2026-68079, CVE-2026-74746, CVE-2026-74744, CVE-2026-74669, CVE-2026-74569, CVE-2026-73194, CVE-2026-72329, CVE-2026-10109, CVE-2026-42584, CVE-2026-42581)
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 Versions - 7.6.0.0 - 7.6.0.5 QRadar Versions - 7.5.0 - 7.5.0 UP16 IF02 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions: • v4.8 • v5.0 • v5.1 • v5.2 • v5.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7295452 • https://www.ibm.com/support/pages/node/7295466

Vendor	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerability (CVE-2026-28336)
Description	Citrix has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-28336:** SolarWinds Dameware was found to be affected by a command injection vulnerability that could lead to the compromise of the remotely controlled host. Authentication is required. Citrix advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	SolarWinds Dameware 2026.3 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28336

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76166, CVE-2026-86247, CVE-2026-78383, CVE-2026-77791, CVE-2026-86350, CVE-2026-76183, CVE-2026-79677, CVE-2026-73581, CVE-2026-86248, CVE-2026-86243, CVE-2026-86246, CVE-2026-43051, CVE-2026-68476, CVE-2026-74669, CVE-2026-74641, CVE-2026-80714, CVE-2026-44432, CVE-2026-11332, CVE-2026-44431, CVE-2026-33814, CVE-2026-39825, CVE-2026-63209, CVE-2026-111943)
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	JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Long Life 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 JBoss Enterprise Web Server 7 for RHEL 10 x86_64 JBoss Enterprise Web Server 7 for RHEL 9 x86_64 JBoss Enterprise Web Server 7 for RHEL 8 x86_64 Red Hat OpenShift Container Platform Red Hat OpenShift Container Platform 4.21 for RHEL 9 x86_64 Red Hat OpenShift Container Platform for Power 4.21 for RHEL 9 ppc64le Red Hat OpenShift Container Platform for IBM Z and LinuxONE 4.21 for RHEL 9 s390x Red Hat OpenShift Container Platform for ARM 64 4.21 for RHEL 9 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:92286 • https://access.redhat.com/errata/RHSA-2026:92995 • https://access.redhat.com/errata/RHSA-2026:92331 • https://access.redhat.com/errata/RHSA-2026:92330 • https://access.redhat.com/errata/RHSA-2026:92994 • https://access.redhat.com/errata/RHSA-2026:92284 • https://access.redhat.com/errata/RHSA-2026:93618 • https://access.redhat.com/errata/RHSA-2026:94596 • https://access.redhat.com/errata/RHSA-2026:93622

Vendor	**SolarWinds**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-28327, CVE-2026-28335)
Description	SolarWinds has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-28327:** SolarWinds Dameware was found to be affected by a DLL hijacking vulnerability. The hijack occurs during installations only and requires access to the local machine and admin privileges. **CVE-2026-28335:** SolarWinds Dameware was found to be affected by a buffer overflow vulnerability that can result in remote code execution. Authentication is required. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Dameware 2026.3 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28327 • https://www.solarwinds.com/trust-center/security-advisories/cve-2026-28335

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-53381, CVE-2026-63968, CVE-2026-64217, CVE-2026-68426, CVE-2026-74469, CVE-2026-74669, CVE-2026-89544, CVE-2026-89551, CVE-2026-89674, CVE-2026-98432)
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 Live Patching 15-SP7 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 15 SP7 SUSE Linux Enterprise Server for SAP Applications 15 SP7 openSUSE Leap 15.4 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise High Performance Computing 12 SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2026/suse-su-20265058-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265059-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265081-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265084-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265085-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265086-1/ • https://www.suse.com/support/update/announcement/2026/suse-su-20265088-1/

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-95722, CVE-2026-95723, CVE-2026-95724, CVE-2026-95725, CVE-2026-95726, CVE-2026-95727, CVE-2026-95728, CVE-2026-95729, CVE-2026-95730, CVE-2026-95734, CVE-2026-95735, CVE-2026-95736, CVE-2026-95737, CVE-2026-95738, CVE-2026-95739, CVE-2026-95740, CVE-2026-95741, CVE-2026-95742, CVE-2026-95743, CVE-2026-95744, CVE-2026-95745, CVE-2026-95746, CVE-2026-95747, CVE-2026-95748, CVE-2026-95749, CVE-2026-95750, CVE-2026-95751, CVE-2026-95752, CVE-2026-95753, CVE-2026-95755, CVE-2026-95756, CVE-2026-95757, CVE-2026-95758, CVE-2026-95759, CVE-2026-95760, CVE-2026-95761, CVE-2026-95762, CVE-2026-95763, CVE-2026-95764, CVE-2026-95765, CVE-2026-95766, CVE-2026-95767, CVE-2026-95768, CVE-2026-95769, CVE-2026-95770, CVE-2026-95771, CVE-2026-95772, CVE-2026-95773, CVE-2026-95774, CVE-2026-95775, CVE-2026-95776, CVE-2026-95777)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	• HPE Networking Fabric Composer (AFC) 7.4.0 and below • HPE Networking Fabric Composer (AFC) 7.3.4 and below • HPE Networking VIA client (all platforms) Versions - 4.7.8 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05173en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05172en_us&docLocale=en_US

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	QRadar Versions - 7.6.0.0 - 7.6.0.5 QRadar Versions - 7.5.0 - 7.5.0 UP16 IF02 IBM Db2 Genius Hub Versions: 1.1.2, 1.1.3, 1.1.4, 1.1.5 Agentics Version - 1.0 IBM Db2 on Cloud Pak for Data and Db2 Warehouse on Cloud Pak for Data Versions: • v4.8 • v5.0 • v5.1 • v5.2 • v5.3 Db2 Query Management Facility Versions: • 13.1.1 • 13.1.2 • 13.1.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7295452 • https://www.ibm.com/support/pages/node/7295466 • https://www.ibm.com/support/pages/node/7295187 • https://www.ibm.com/support/pages/node/7295404

Vendor	**NetApp**
Severity	**Medium**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-22060)
Description	NetApp has released a security update addressing a vulnerability that exists in their products. **CVE-2026-22060:** ll versions of StorageGRID (formerly StorageGRID Webscale) in default & common configurations allow an unauthenticated attacker to access a limited set of APIs that are intended for use within the grid. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	StorageGRID (formerly StorageGRID Webscale)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261103-0002

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.