Advisory Alert

Alert Number: AAA20261019 **Date:** October 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Vendor	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-80441, CVE-2026-80442, CVE-2026-84075, CVE-2026-84078, CVE-2026-81657, CVE-2026-84082, CVE-2026-84073, CVE-2026-84436, CVE-2026-82340, CVE-2026-84031, CVE-2026-84064)
Description	IBM 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. 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 & 12.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288040

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-102994, CVE-2026-102998, CVE-2026-31772, CVE-2026-43020, CVE-2026-43450, CVE-2026-46149, CVE-2026-46189, CVE-2026-63920, CVE-2026-63922, CVE-2026-63924, CVE-2026-63984, CVE-2026-63993, CVE-2026-64113, CVE-2026-64490, CVE-2026-68086, CVE-2026-68480, CVE-2026-80792, CVE-2026-98260, CVE-2026-31411)
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 Quay Red Hat Enterprise Linux 6: • Extended Life Cycle Support Extension (ELCS): i386, s390x, x86_64 Red Hat Enterprise Linux 9: • 9.2:Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, x86_64) • 9.4: Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), 4 Years of Updates (aarch64, s390x), Update Services for SAP Solutions (ppc64le, 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) Red Hat Enterprise Linux 10: • 10.0: Extended Update Support (EUS) & CodeReady Linux Builder EUS (all archs), 4 Years of Updates / Support (all archs)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:83822 https://access.redhat.com/errata/RHSA-2026:83707 https://access.redhat.com/errata/RHSA-2026:83738 https://access.redhat.com/errata/RHSA-2026:83775 https://access.redhat.com/errata/RHSA-2026:83796 https://access.redhat.com/errata/RHSA-2026:83797

Vendor	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-5121, CVE-2026-4111, CVE-2026-4424)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-5121:** Libarchive versions 2.8.0 through 3.8.6 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. **CVE-2026-4111:** Libarchive versions prior to 3.8.6 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2026-4424:** Libarchive versions 3.6.0 through 3.8.6 are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ONTAP tools for VMware vSphere 10 ONTAP 9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261016-0005 https://security.netapp.com/advisory/ntap-20261016-0006 https://security.netapp.com/advisory/ntap-20261016-0007

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 Infrastructure: SUSE Linux Enterprise 15 SP7: Basesystem Module, Desktop, Development Tools Module, High Availability Extension, Legacy Module, Live Patching, Public Cloud Module, Real Time, Server, Server for SAP Applications, Workstation Extension
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20264702-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264693-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264708-1/ https://www.suse.com/support/update/announcement/2026/suse-su-20264706-1/

Vendor	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84862, CVE-2026-84071, CVE-2026-81669, CVE-2026-81937, CVE-2026-81656, CVE-2026-84034, CVE-2026-81626, CVE-2026-81933, CVE-2026-81623, CVE-2026-102278, CVE-2026-102277, CVE-2026-102276, CVE-2026-81870, CVE-2026-17495, CVE-2026-93749)
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 & 12.1 IBM Security QRadar Log Management AQL Plugin versions 1.0.0 - 1.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7288040 https://www.ibm.com/support/pages/node/7292917

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.