Advisory Alert

Alert Number: AAA20261012 **Date:** October 12, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Authentication Bypass Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
NetApp	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
MongoDB	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Dell	**Medium**	Multiple Vulnerabilities

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2026-79842)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-79842:** A potential security vulnerability has been identified in HPE Intelligent Management Center (iMC). The vulnerability could remotely exploited to allow authentication bypass. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Intelligent Management Center Version 7.3 E0713
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05157en_us&docLocale=en_US

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-74705, CVE-2026-46149, CVE-2026-63802, CVE-2026-64320, CVE-2026-72129)
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 Enterprise Linux 8: • 8.4 & 8.6: Advanced Update Support (AUS): x86_64 • 8.4, 8.6 & 8.8: Extended Life Cycle Long Life: x86_64 • 8.8: Update Services for SAP Solutions (ppc64le, x86_64), Update Services (TUS): x86_64 Red Hat Enterprise Linux 9: • 9.4: 4 Years of Updates (aarch64, s390x), Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), Update Services for SAP Solutions (ppc64le, x86_64) • 9.6: 4 Years of Updates (aarch64, s390x), Advanced Update Support (AUS) (x86_64), Extended Life Cycle (all archs), Extended Update Support (EUS) & CodeReady Linux Builder EUS (all archs), 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-2026:79786 https://access.redhat.com/errata/RHSA-2026:79784 https://access.redhat.com/errata/RHSA-2026:79783 https://access.redhat.com/errata/RHSA-2026:79782 https://access.redhat.com/errata/RHSA-2026:79778

Vendor	**NetApp**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-46600, CVE-2026-22061)
Description	NetApp has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-46600:** Golang.Org/X/Net versions prior to 0.56.0 are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service (DoS). **CVE-2026-22061:** Trident versions v25.02.1 through v26.06.1 are susceptible to a vulnerability that could allow an authenticated attacker with access to debug logs to view LUKS passphrases or SMB Active Directory credentials. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetApp Infrastructure: • NetApp Console Agent Container (tp-proxy) • Trident Protect Connector • Trident
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20261009-0025 https://security.netapp.com/advisory/ntap-20261009-0026

Vendor	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-78002, CVE-2026-14532, CVE-2026-14909, CVE-2026-79715, CVE-2026-77816, CVE-2026-11713)
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	AIX versions 7.2 and 7.3 VIOS version 4.1 IBM WebSphere Hybrid Edition version 5.1 IBM WebSphere Application Server Liberty version 17.0.0.3 - 26.0.0.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7291353 https://www.ibm.com/support/pages/node/7291353 https://www.ibm.com/support/pages/node/7291873

Vendor	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-6052, CVE-2026-0861, CVE-2026-94579, CVE-2026-87660, CVE-2026-87674, CVE-2026-87688, CVE-2026-94585, CVE-2026-87663, CVE-2026-87664, CVE-2026-87685, CVE-2021-4083, CVE-2026-1484, CVE-2026-87679, CVE-2026-94575, CVE-2026-87659, CVE-2026-87686, CVE-2026-94583, CVE-2026-87671, CVE-2026-94578)
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 Brocade Fabric OS - Versions before Brocade Fabric OS 9.2.2d and 10.0.0 - 10.0.0a1 HPE Brocade Fabric OS - Versions before v10.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst05161en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbst05160en_us&docLocale=en_US

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 Versions 24.04 and 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8887-3 https://ubuntu.com/security/notices/USN-8911-1 https://ubuntu.com/security/notices/USN-8875-2 https://ubuntu.com/security/notices/USN-8903-2 https://ubuntu.com/security/notices/USN-8905-2

Vendor	**MongoDB**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-87109, CVE-2026-87108, CVE-2026-87110, CVE-2026-106435, CVE-2026-106436, CVE-2026-106432, CVE-2026-107325, CVE-2026-107324, CVE-2026-106434, CVE-2026-106433, CVE-2026-106429, CVE-2026-106430, CVE-2026-106438, CVE-2026-106437, CVE-2026-106431, CVE-2026-106428)
Description	MongoDB 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. MongoDB advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	MongoDB Infrastructure: C Driver: • 1.4.0 (affects versions prior to 1.30.13) • 0.5.0 (affects versions prior to 1.30.13) • 2.0.0 (affects versions prior to 2.4.0, 2.5.6) C++ Driver: • 3.0.0 (affects versions prior to 4.6.1) libmongocrypt: • 1.5.0 (affects versions prior to 1.20.5) Go Driver: • (affects versions prior to 1.2.0) • (affects 1.17.10 and prior versions) • 2.0.0 (affects versions prior to 2.9.0, 2.9.2) PHP Driver: • 1.3.0 – 1.16.0 (affects versions prior to 1.21.11) • 2.0.0 (affects versions prior to 2.1.11) • 2.2.0 (affects versions prior to 2.5.4) Python Driver: • 0.10.3 (affects 4.18.2 and prior versions) Ops Manager: • 7.0.0 (affects 7.0.23 and prior versions) • 8.0.0 (affects versions prior to 8.0.27)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.mongodb.com/resources/products/alerts#security

Vendor	**Dell**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-35161, CVE-2026-94348)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-35161:** Dell PowerScale InsightIQ, versions 5.2.0 through 6.3.0, contains an Overly Restrictive Account Lockout Mechanism vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Denial of service. **CVE-2026-94348:** Dell PowerScale InsightIQ, versions 5.2.0 through 6.3.0, contains an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale InsightIQ Versions 5.2.0 through 6.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000518964/dsa-2026-439-security-update-for-dell-powerscale-insightiq-multiple-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.