Advisory Alert

Alert Number: AAA20260220 **Date:** February 20, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Uncontrolled Search Path Element Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Denial of Service (DoS) Vulnerability

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Uncontrolled Search Path Element Vulnerability (CVE-2026-21420)
Description	Dell has released security updates addressing a vulnerability that exists in their products. **CVE-2026-21420** - an Uncontrolled Search Path Element vulnerability that allows a low privileged attacker with local access to potentially exploit this vulnerability, leading to arbitrary code execution and escalation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Repository Manager Versions prior to 3.4.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000430183/dsa-2026-059-security-update-for-dell-repository-manager-vulnerability

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-13867, CVE-2025-36247, CVE-2025-36425, CVE-2025-62230, CVE-2025-62231, CVE-2025-13333)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Remote Server Versions 9.0 and 9.1 IBM WebSphere Remote Server Versions 8.5, 9.0, and 9.1 AIX versions 7.2 and 7.3 VIOS version 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7261318 • https://www.ibm.com/support/pages/node/7261316 • https://www.ibm.com/support/pages/node/7261396

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20064, CVE-2025-20068, CVE-2025-20105, CVE-2025-20028, CVE-2025-20027, CVE-2025-22444, CVE-2025-22850, CVE-2025-20073, CVE-2025-31648)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE SimpliVity 380 Gen10 - Prior to SimpliVity Support Pack (SVTSP) Gen10 2026-0116 HPE SimpliVity 380 Gen10 G - Prior to SimpliVity Support Pack (SVTSP) Gen10 2026-0116 HPE SimpliVity 380 Gen10 H - Prior to SimpliVity Support Pack (SVTSP) Gen10 2026-0116 HPE SimpliVity 380 Gen10 Plus - Prior to SimpliVity Support Pack (SVTSP) Gen10 2026-0116 HPE SimpliVity 380 Gen11 - Prior to SimpliVity Support Pack (SVTSP) Gen11 2026-0116 HPE StoreEasy 1470 Performance - Prior to v2.80_01-29-2026 (U63 ROM Family) HPE StoreEasy 1470 Storage - Prior to v2.80_01-29-2026 (U63 ROM Family) HPE StoreEasy 1570 Performance - Prior to v2.80_01-29-2026 (U63 ROM Family) HPE StoreEasy 1570 Storage - Prior to v2.80_01-29-2026 (U63 ROM Family) HPE StoreEasy 1670 Performance Storage - Prior to v2.80_01-29-2026 (U54 ROM Family) HPE StoreEasy 1670 Storage - Prior to v2.80_01-29-2026 (U54 ROM Family) HPE StoreEasy 1870 Performance Storage - Prior to v2.80_01-29-2026 (U54 ROM Family) HPE StoreEasy 1870 Storage - Prior to v2.80_01-29-2026 (U54 ROM Family) HPE StoreEasy 1660 Storage - Prior to v2.60_02-05-2026 (U46 ROM Family) HPE StoreEasy 1860 Storage - Prior to v2.60_02-05-2026 (U46 ROM Family) HPE StoreEasy 1670 Expanded Storage - Prior to v2.60_02-05-2026 (U50 ROM Family)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf05016en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04967en_us&docLocale=en_US

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Denial of Service (DoS) Vulnerability (CVE-2022-23023)
Description	F5 has released security updates addressing a vulnerability that exists in the iControl REST of their products. **CVE-2022-23023** - undisclosed requests by an authenticated iControl REST user can cause an increase in memory resource utilization. This vulnerability allows an authenticated remote attacker to cause a degradation of service that can lead to a denial-of-service (DoS). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IQ Centralized Management versions through 8.0.0 - 8.4.0 BIG-IP (all modules) versions through: • 16.1.0 - 16.1.2 • 15.1.0 - 15.1.4 • 14.1.0 - 14.1.4 • 13.1.0 - 13.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K11742742

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.