Advisory Alert

Alert Number: AAA20260219 **Date:** February 19, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
F5	**High**	Denial of Service Vulnerability
Ivanti	**High**, Medium	Multiple Vulnerabilities
IBM	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released a security update addressing multiple vulnerabilities that exist in the Power Protect Data Manager product. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell PowerProtect Data Manager versions prior to 19.22.0-24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000429778/dsa-2026-046-security-update-for-dell-powerprotect-data-manager-multiple-vulnerabilities

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2026-2507)
Description	F5 has released a security update addressing a vulnerability that exists in their products. **CVE-2026-2507**: Traffic is disrupted while the TMM process restarts. This vulnerability allows a remote, unauthenticated attacker to cause a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only. F5 advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	BIG-IP AFM and DDoS Hybrid Defender versions 17.5.1.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000160003

Affected Product	**Ivanti**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-1602, CVE-2026-1603)
Description	Ivanti has released a security update addressing multiple vulnerabilities that exist in Ivanti Endpoint Manager (EPM). **CVE-2026-1602**: SQL injection in Ivanti Endpoint Manager before version 2024 SU5 allows a remote authenticated attacker to read arbitrary data from the database. **CVE-2026-1603**: An authentication bypass in Ivanti Endpoint Manager before version 2024 SU5 allows a remote unauthenticated attacker to leak specific stored credential data. Ivanti advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ivanti Endpoint Manager (EPM) versions 2024 SU4 SR1 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://hub.ivanti.com/s/article/Security-Advisory-EPM-February-2026-for-EPM-2024?language=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-13333, CVE-2025-40778, CVE-2025-40780, CVE-2025-8677, CVE-2025-8732)
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 WebSphere Hybrid Edition versions 5.1 IBM WebSphere Application Server versions 8.5 and 9.0 AIX versions 7.2 and 7.3 VIOS versions 4.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7261249 • https://www.ibm.com/support/pages/node/7261171 • https://www.ibm.com/support/pages/node/7261170

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.