Advisory Alert

Alert Number: AAA20260603 **Date:** June 3, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
HPE	**High**	Side-Channel Timing Attack
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell 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. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Private Cloud -VMware Versions prior to 01.04.00.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000472451/dsa-2026-242-security-update-for-dell-private-cloud-vmware-for-multiple-third-party-component-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-9319, CVE-2026-1525, CVE-2026-4800, CVE-2026-39892, CVE-2025-62718, CVE-2026-29063, CVE-2023-46233, CVE-2026-1188, CVE-2026-1346)
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 Security QRadar EDR versions 3.12 - 3.12.24 • IBM WebSphere Remote Server versions 8.5, 9.0, and 9.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7274827 • https://www.ibm.com/support/pages/node/7274859

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Side-Channel Timing Attack (CVE-2024-39894)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. CVE-2024-39894 - A vulnerability in OpenSSH's ObscureKeystrokeTiming feature (introduced in version 9.5) renders its keystroke timing obfuscation ineffective due to a logic error. This may allow attackers to observe keystroke timing patterns despite the feature being enabled by default. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	HPE Aruba Networking ArubaOS-CX Switches • 10.16.1000 and below • 10.15.0005 and below • 10.13.1080 and below • 10.10.1150 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05062en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45636, CVE-2025-12635, CVE-2025-13465, CVE-2025-47913, CVE-2025-47914, CVE-2025-58181, CVE-2026-1342, CVE-2026-1343, CVE-2026-1345, CVE-2026-1491, CVE-2026-1526, CVE-2026-1527, CVE-2026-1528, CVE-2026-2229, CVE-2026-2359, CVE-2026-2475, CVE-2026-2581, CVE-2026-2862, CVE-2026-2950, CVE-2026-3304, CVE-2026-4101, CVE-2026-4364, CVE-2026-21925, CVE-2026-21932, CVE-2026-21933, CVE-2026-21945, CVE-2026-22036, CVE-2026-24486, CVE-2026-25645, CVE-2026-26007, CVE-2026-30951, CVE-2026-31533, CVE-2026-32286, CVE-2026-33151, CVE-2026-33532, CVE-2026-33671, CVE-2026-33672, CVE-2026-33750, CVE-2026-33870, CVE-2026-33871, CVE-2026-34477, CVE-2026-34478, CVE-2026-34479, CVE-2026-34480, CVE-2026-39373, CVE-2026-40175)
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 Verify Identity Access Container versions 10.0 - 10.0.91 and 11.0 - 11.0.2 IBM Verify Identity Access versions 10.0 - 10.0.9.1 and 11.0 - 11.0.2 IBM Security QRadar EDR versions 3.12 - 3.12.24
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7268253 • https://www.ibm.com/support/pages/node/7274828 • https://www.ibm.com/support/pages/node/7274827

Affected Product	**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 26.04 LTS, 25.0, 24.04 LTS, 22.04 LTS, 14.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-8361-1 • https://ubuntu.com/security/notices/USN-8370-1 • https://ubuntu.com/security/notices/USN-8371-1 • https://ubuntu.com/security/notices/USN-8373-1 • https://ubuntu.com/security/notices/USN-8374-1

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.