Advisory Alert

Alert Number: AAA20251203 **Date:** December 3, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-36251, CVE-2025-36096, CVE-2025-36250, CVE-2025-7783)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Use Case Manager app and Virtual products. These vulnerabilities could be exploited by malicious users to cause Arbitrary Commands Execution, HTTP Parameter Pollution and gain unauthorized access. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1 IBM QRadar Use Case Manager app versions 1.0.0 - 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7251173 • https://www.ibm.com/support/pages/node/7253432

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerStoreT OS. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerStoreT OS versions prior to 4.3.0.0-2611831 of: PowerStore 500T, PowerStore 1000T, PowerStore 1200T, PowerStore 3000T, PowerStore 3200Q, PowerStore 3200T, PowerStore 5000T, PowerStore 5200Q, PowerStore 5200T, PowerStore 7000T, PowerStore 9000T, PowerStore 9200T
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000399092/dsa-2025-429-dell-powerstore-t-security-update-for-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-20149, CVE-2024-12905, CVE-2024-45296, CVE-2024-47764, CVE-2024-52798, CVE-2024-55565, CVE-2025-5889, CVE-2025-7338, CVE-2025-7339, CVE-2025-12758, CVE-2025-27152, CVE-2025-27789, CVE-2025-46653, CVE-2025-47935, CVE-2025-47944, CVE-2025-48387, CVE-2025-48997, CVE-2025-56200, CVE-2025-57350, CVE-2025-58754, CVE-2025-59343, CVE-2025-36236)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM QRadar Use Case Manager app and Virtual products. These vulnerabilities could be exploited by malicious users to cause Directory Traversal, Denial of Service, Data Modification, Memory Leak. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	AIX versions 7.2 and 7.3 VIOS versions 3.1 and 4.1 IBM QRadar Use Case Manager app versions 1.0.0 - 4.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7251173 • https://www.ibm.com/support/pages/node/7253432

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-14040, CVE-2019-8331, CVE-2019-11358, CVE-2020-7676, CVE-2025-7783, CVE-2025-54419, CVE-2025-58754)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in HPE Unified OSS Console Assurance Monitoring. These vulnerabilities could be exploited by malicious users to cause Authentication Bypass, Input Validation, Local and Remote Code Execution. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Telco Unified OSS Console - Prior to v3.1.17
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04974en_us&docLocale=en_US

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.