Advisory Alert

Alert Number: **AAA20251222** **Date:** **December 22, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Hitachi	**High**	Multiple Vulnerabilities
IBM	**High, Medium**	Multiple Vulnerabilities
Red Hat	**High, Medium**	Multiple Vulnerabilities
Dell	**Medium**	Integrity Check Bypass Vulnerability

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 system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000402262/dsa-2025-425-dell-powermaxos-dell-powermax-eem-dell-unisphere-for-powermax-dell-unisphere-for-powermax-virtual-appliance-dell-unisphere-360-dell-solutions-enabler-virtual-appliance-security-update-for-multiple-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000405611/dsa-2025-455-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000405813/dsa-2025-415-security-update-for-dell-powerprotect-data-domain-multiple-vulnerabilities

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-7783, CVE-2025-9288, CVE-2025-29927, CVE-2025-55182)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause remote code execution, data manipulation, authorization check bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Analyst Workflow versions 2.32.0 - 3.0.0 IBM QRadar Network Threat Analytics app versions 1.3.1 - 1.4.1 IBM QRadar User Behavior Analytics versions 4.1.15 - 5.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7255495 • https://www.ibm.com/support/pages/node/7255496 • https://www.ibm.com/support/pages/node/7255497

Affected Product	**Hitachi**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55248, CVE-2025-59505, CVE-2025-59506, CVE-2025-59507, CVE-2025-59508, CVE-2025-59509, CVE-2025-59510, CVE-2025-59511, CVE-2025-59512, CVE-2025-59513, CVE-2025-59514, CVE-2025-59515, CVE-2025-60703, CVE-2025-60704, CVE-2025-60705, CVE-2025-60706, CVE-2025-60707, CVE-2025-60708, CVE-2025-60709, CVE-2025-60714, CVE-2025-60715, CVE-2025-60716, CVE-2025-60717, CVE-2025-60719, CVE-2025-60720, CVE-2025-60723, CVE-2025-60724, CVE-2025-62208, CVE-2025-62209, CVE-2025-62213, CVE-2025-62215, CVE-2025-62217, CVE-2025-62218, CVE-2025-62219, CVE-2025-62452)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in third party products which affect Hitachi Disk Array Systems. These vulnerabilities could be exploited by malicious users to compromise the affected system. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5600, 5600H, 5500, 5500H, 5200, 5200H, 5100, 5100H
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2025/11.html

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-21587, CVE-2025-27789, CVE-2025-30698, CVE-2025-4447, CVE-2025-47279, CVE-2025-48068, CVE-2025-53057, CVE-2025-53066, CVE-2025-54798, CVE-2025-55173, CVE-2025-55183, CVE-2025-55184, CVE-2025-57752, CVE-2025-57822, CVE-2025-5889, CVE-2025-64756, CVE-2025-67779)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause arbitrary code execution, data modification, information disclosure, denial of service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar Analyst Workflow versions 2.32.0 - 3.0.0 IBM QRadar Network Threat Analytics app versions 1.3.1 - 1.4.1 IBM QRadar User Behavior Analytics versions 4.1.15 - 5.0.2 IBM WebSphere Service Registry and Repository Studio versions 8.5 to 8.5.6.3 IBM WebSphere Service Registry and Repository versions 8.5 to 8.5.6.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7255495 • https://www.ibm.com/support/pages/node/7255496 • https://www.ibm.com/support/pages/node/7255497 • https://www.ibm.com/support/pages/node/7255410

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38499, CVE-2025-39843, CVE-2025-39925)
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 system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.6 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.6 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.6 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.6 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.6 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.6 ppc64le Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.6 x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux Server - AUS 9.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.6 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:23730 • https://access.redhat.com/errata/RHSA-2025:23789

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Integrity Check Bypass Vulnerability (CVE-2023-48795)
Description	Dell has released security updates addressing an Integrity Check Bypass Vulnerability that exists in OpenSSH which affects Dell NetWorker Virtual Edition. **CVE-2023-48795** – This vulnerability allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Networker Virtual Edition versions prior to 19.13
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000405768/dsa-2025-450-security-update-for-dell-networker-virtual-edition-openssl-vulnerability

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.