Advisory Alert

Alert Number: AAA20240405 **Date:** April 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Container Breakout Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Apache	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has issued security updates addressing Multiple Vulnerabilities that exist in Dell PowerStore X. If exploited, these vulnerabilities could lead to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerStore 1000X running on PowerStoreX OS versions prior to 3.2.1.2-2265367 PowerStore 3000X running on PowerStoreX OS versions prior to 3.2.1.2-2265367 PowerStore 5000X running on PowerStoreX OS versions prior to 3.2.1.2-2265367 PowerStore 7000X running on PowerStoreX OS versions prior to 3.2.1.2-2265367 PowerStore 9000X running on PowerStoreX OS versions prior to 3.2.1.2-2265367
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223810/dsa-2024-158-dell-powerstore-x-security-update-for-multiple-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1973, CVE-2023-4639, CVE-2023-48795, CVE-2024-1635)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-1973 -** A flaw was found in Undertow package. Using the FormAuthenticationMechanism, a malicious user could trigger a Denial of Service by sending crafted requests, leading the server to an OutofMemory error, exhausting the server's memory. **CVE-2023-4639 -** A flaw was found in Undertow, which incorrectly parses cookies with certain value-delimiting characters in incoming requests. This issue could allow an attacker to construct a cookie value to exfiltrate HttpOnly cookie values or spoof arbitrary additional cookie values, leading to unauthorized data access or modification. The main threat from this flaw impacts data confidentiality and integrity. **CVE-2023-48795 -** A flaw was found in the SSH channel integrity. By manipulating sequence numbers during the handshake, an attacker can remove the initial messages on the secure channel without causing a MAC failure. For example, an attacker could disable the ping extension and thus disable the new countermeasure in OpenSSH 9.5 against keystroke timing attacks. **CVE-2024-1635 -** A flaw was found in Undertow which impacts a server that supports the wildfly-http-client protocol. Whenever a malicious user opens and closes a connection with the HTTP port of the server and then closes the connection immediately, the server will end with both memory and open file limits exhausted at some point, depending on the amount of memory available. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 9 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 8 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:1677 • https://access.redhat.com/errata/RHSA-2024:1676 • https://access.redhat.com/errata/RHSA-2024:1675 • https://access.redhat.com/errata/RHSA-2024:1674

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Container Breakout Vulnerability (CVE-2024-21626)
Description	Dell has released security updates addressing a Container breakout vulnerability that exists in runc CLI which used in Dell NetWorker vProxy OVA. **CVE-2024-21626 - Due** to an internal file descriptor leak, an attacker could cause a newly-spawned container process (from runc exec) to have a working directory in the host filesystem namespace, allowing for a container escape by giving access to the host filesystem. Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell NetWorker vProxy- vProxy OVA Versions 9.10 prior to 19.10.0.2 Dell NetWorker vProxy- vProxy OVA Versions prior to 19.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223801/dsa-2024-164-security-update-for-dell-networker-vproxy-runc-component-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20373, CVE-2023-38729, CVE-2024-27268, CVE-2023-50313, CVE-2023-51775)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Information Disclosure and Denial of service IBM recommends to apply security fixes at your earliest to protect your systems from potential threats.
Affected Products	IBM Db2 10.1.0.x Server IBM Db2 10.5.0.x Server IBM Db2 11.1.4.x Server IBM Db2 11.5.x Server IBM Db2 9.7.0.x Server IBM WebSphere Application Server 8.5 IBM WebSphere Application Server 9.0 IBM WebSphere Application Server Liberty 18.0.0.2 - 24.0.0.3 IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Remote Server 9.0, 8.5 WebSphere Service Registry and Repository 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/6523804 • https://www.ibm.com/support/pages/node/7145721 • https://www.ibm.com/support/pages/node/7145918 • https://www.ibm.com/support/pages/node/7145936 • https://www.ibm.com/support/pages/node/7145942 • https://www.ibm.com/support/pages/node/7145905

Affected Product	**Apache**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-38709, CVE-2024-24795, CVE-2024-27316)
Description	Apache has released security updates addressing multiple vulnerabilities that exist in Apache HTTP Server. **CVE-2023-38709 –** Vulnerability in Faulty input validation in the core of Apache allows malicious or exploitable backend/content generators to split HTTP responses. **CVE-2024-24795 –** Vulnerability in HTTP Response splitting in multiple modules in Apache HTTP Server allows an attacker that can inject malicious response headers into backend applications to cause an HTTP desynchronization attack. **CVE-2024-27316 -** Vulnerability in HTTP/2 incoming headers exceeding the limit are temporarily buffered in nghttp2 in order to generate an informative HTTP 413 response. If a client does not stop sending headers, this leads to memory exhaustion. Apache advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache HTTP Server versions below 2.4.59
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.