



Advisory Alert

Alert Number: AAA20240305

Date: March 5, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	Critical	Multiple Vulnerabilities
IBM	Critical	Arbitrary Code Execution Vulnerability
Dell	High	Multiple Vulnerabilities
IBM	High, Medium, Low	Multiple Vulnerabilities
F5	Medium	OpenLDAP Vulnerability

Description

Affected Product	Dell
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2022-43505, CVE-2022-40982, CVE-2022-36763, CVE-2022-36764, CVE-2023-32460)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell PowerScale OneFS. Dell PowerScale OneFS remediation is available for multiple security vulnerabilities in node firmware that could be exploited by malicious users to compromise the affected system. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerScale Node Firmware Package Versions prior to 12.1 in <ul style="list-style-type: none"> Isilon A200 Isilon A2000 PowerScale Archive A300 PowerScale Archive A3000 Isilon H400 Isilon H500 Isilon H600 Isilon H5600 PowerScale Hybrid H700 PowerScale Hybrid H7000 PowerScale B100 PowerScale F200 PowerScale F600 Isilon F800 PowerScale F900 PowerScale P100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222692/dsa-2024-090-security-update-for-dell-powerscale-onefs-for-multiple-security-vulnerabilities

Affected Product	IBM
Severity	Critical
Affected Vulnerability	Arbitrary code execution vulnerability (CVE-2023-40743)
Description	IBM has released a security update addressing an Arbitrary code execution vulnerability, caused by improper input validation by the ServiceFactory.getService function. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code, cause a denial of service or perform SSRF attacks. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	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/7129833

Affected Product	Dell
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22463, CVE-2024-24901, CVE-2022-2827, CVE-2022-26872)
Description	Dell has released a security update addressing multiple vulnerabilities. An attacker may exploit these vulnerabilities to cause Sensitive information disclosure, User Enumeration, Password reset interception via API. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PowerScale OneFS <ul style="list-style-type: none"> • Version 9.6.1.0 • Versions 8.2.0 through 9.2.1.24 • Versions 8.2.0 through 9.4.0.16 • Versions 9.3.0.0 through 9.4.0.16 • Versions 9.5.0.0 through 9.5.0.5 • Versions 9.5.0.0 through 9.5.0.6 PowerSwitch S5448F-ON - BMC before 4.52.6.4-3.03 PowerSwitch Z9432F-ON - BMC before 3.06 PowerSwitch Z9664F-ON - BMC before 4.54.6.4-2.03
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222691/dsa-2024-062-security-update-for-dell-powerscale-onefs-for-proprietary-code-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000222696/dsa-2024-116-dell-emc-networking-security-update-for-multiple-vulnerabilities

Affected Product	IBM
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-40743, CVE-2022-41854, CVE-2022-38752, CVE-2022-38751, CVE-2022-38750, CVE-2022-38749, CVE-2022-25857, CVE-2022-1471, CVE-2023-34478, CVE-2024-20952, CVE-2024-20918, CVE-2024-20921, CVE-2024-20945, CVE-2023-33850)
Description	IBM has released security updates for their products. Exploitation of these vulnerabilities may lead to Arbitrary code execution, Denial of Service and Sensitive information disclosure. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	WebSphere Service Registry and Repository 8.5 WebSphere Service Registry and Repository Studio 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7129821 https://www.ibm.com/support/pages/node/7129833

Affected Product	F5
Severity	Medium
Affected Vulnerability	OpenLDAP Vulnerability (CVE-2023-2953)
Description	F5 has released security updates addressing an OpenLDAP vulnerability. The vulnerability causes a null pointer dereference in ber_memalloc_x() function. Exploitation of the vulnerability may result in low system memory leading to failure in LDAP authentication. F5 recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	BIG-IP (all modules) 17.1.0 - 17.1.1, 16.1.0 - 16.1.4, 15.1.0 - 15.1.10 F5OS-A 1.7.0, 1.5.0 - 1.5.1, 1.4.0, 1.3.0 - 1.3.2 F5OS-C 1.6.0 - 1.6.2, 1.5.0 - 1.5.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000138814

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.