FINCSIRT

Advisory Alert

Alert Number: **AAA20241021** **Date:** **October 21, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
NetApp	**High**	Use-after-free Vulnerability
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Out-of-bounds memory write Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in third-party products which in turn affect Dell 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	Dell Storage Resource Manager Versions prior to 5.0.2.0 in Vapp Dell Storage Resource Manager Versions prior to 5.0.2.0 in Windows/Linux update
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000235152/dsa-2024-421-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities

Affected Product	**NetApp**
Severity	**High**
Affected Vulnerability	Use-after-free Vulnerability (CVE-2024-36886)
Description	NetApp has released security updates addressing a Use-after-free Vulnerability that exists in Linux Kernel which is incorporated by NetApp products. **CVE-2024-36886** - Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to disclosure of sensitive information, addition or modification of data, or Denial of Service (DoS). NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	E-Series SANtricity OS Controller Software 11.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.netapp.com/advisory/ntap-20241018-0002/

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5678, CVE-2024-0727, CVE-2024-38320, CVE-2024-21094, CVE-2024-21085, CVE-2024-21011, CVE-2023-38264, CVE-2024-6197, CVE-2024-22354, CVE-2023-38546, CVE-2024-3933, CVE-2024-6874)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause XML External Entity Injections, Denial of Service, Security restriction bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect Backup-Archive Client 8.1.0.0 - 8.1.23.0 IBM Storage Protect for Space Management 8.1.0.0 - 8.1.23.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173465 • https://www.ibm.com/support/pages/node/7173463

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-21781, CVE-2023-43626, CVE-2023-42772, CVE-2024-21871, CVE-2024-23599, CVE-2024-21829)
Description	F5 has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of service, Privilege escalation. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS-A versions 1.7.0 - 1.8.0 and 1.5.1 - 1.5.2 F5OS-C versions 1.6.0 - 1.6.2 BIG-IP (all modules) versions 17.1.0 - 17.1.1, 16.1.0 - 16.1.5 and 15.1.0 - 15.1.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://my.f5.com/manage/s/article/K000141509 • https://my.f5.com/manage/s/article/K000141511 • https://my.f5.com/manage/s/article/K000141503 • https://my.f5.com/manage/s/article/K000141501 • https://my.f5.com/manage/s/article/K000141500 • https://my.f5.com/manage/s/article/K000141505

Affected Product	**OpenSSL**
Severity	**Low**
Affected Vulnerability	Out-of-bounds memory write Vulnerability (CVE-2024-9143)
Description	OpenSSL has released security updates addressing an Out-of-bounds memory write Vulnerability that exists in their products. **CVE-2024-9143** - Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. OpenSSL advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSSL Versions 3.3, 3.2, 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/secadv/20241016.txt

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.