Advisory Alert

Alert Number: **AAA20230208** **Date:** **February 8, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
OpenSSL	**High, Medium**	Multiple Vulnerabilities
Dell	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**OpenSSL**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0286, CVE-2022-4304, CVE-2022-4203, CVE-2023-0215, CVE-2022-4450, CVE-2023-0216, CVE-2023-0217, CVE-2023-0401)
Description	OpenSSL has released a security updates to address multiple vulnerabilities that exist in the openSSL libraries. Using these vulnerabilities an attacker can launch denial of service attacks, read memory contents, sensitive data exposure and system crash. OpenSSL recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	OpenSSL versions 1.1.1, 1.0.2, 3.0.0 to 3.0.7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230207.txt

Affected Product	**Dell**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0144, CVE-2023-24573, CVE-2023-24572, CVE-2023-23697)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to privilege escalation and arbitrary folder deletion. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell Command | Monitor Versions before 10.9 Dell Command | Integration Suite for System Center Versions prior to 6.4.0 Dell Command | Intel vPro Out of Band Versions before 4.4.0 VEP4600-16 Core X722 FW before version 5.0 VEP4600-8 Core X722 FW before version 5.0 VEP4600-4 Core X722 FW before version 5.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000207973/dsa-2023-033 https://www.dell.com/support/kbdoc/en-us/000207931/dsa-2023-032 https://www.dell.com/support/kbdoc/en-us/000207929/dsa-2023-030 https://www.dell.com/support/kbdoc/en-us/000208398/dsa-2023-062-dell-emc-networking-security-update-for-a-third-party-bios-vulnerability

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.