Advisory Alert

Alert Number: **AAA20230323** **Date:** **March 23, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Cisco	**High, Medium**	Multiple Vulnerabilities
OpenSSL	**Low**	Denial Of Service Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-37434, CVE-2018-25032, CVE-2022-29885, CVE-2022-34305, CVE-2022-40674, CVE-2022-25235, CVE-2022-25236, CVE-2022-25315, CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-22852, CVE-2021-43527, CVE-2021-3695, CVE-2021-3696, CVE-2021-3697, CVE-2022-28733, CVE-2022-28734, CVE-2022-28736)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of the most severe vulnerabilities could lead to heap-based buffer overflow, memory corruption, Denial of Service and Cross site scripting. Dell highly recommends applying necessary fixes to avoid issues.
Affected Products	Dell PowerProtect DD DDOS and DDMC versions 7.0 to 7.10 and version 6.2.1.90 and below Dell PowerProtect DD SmartScale version 7.8 to 7.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000211365/dsa-2023-110-dell-technologies-powerprotect-dd-security-update-for-multiple-security-vulnerabilities

Affected Product	**Cisco**
Severity	**High, Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-20027, CVE-2023-20065, CVE-2023-20035, CVE-2023-20072, CVE-2023-20080, CVE-2023-20067, CVE-2023-20055, CVE-2023-20082, CVE-2023-20112, CVE-2023-20066, CVE-2023-20113, CVE-2023-20029, CVE-2023-20059, CVE-2023-20100, CVE-2023-20081, CVE-2023-20107, CVE-2023-20056, CVE-2023-20097)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited, these vulnerabilities could lead to Denial of Service, Privilege Escalation, command injection, UI path traversal, Cross-Site Request Forgery, Low-Entropy Keys, and Information disclosure. Cisco recommends to apply necessary fixes to avoid issues.
Affected Products	1000 Series Integrated Services Routers 4000 Series Integrated Services Routers 6300 Series Embedded Services APs Aironet 1540 Series APs Aironet 1560 Series APs Aironet 1800 Series APs Aironet 2800 Series APs Aironet 3800 Series APs Aironet 4800 APs ASA 5506H-X Security Appliances ASA 5506W-X Security Appliances ASA 5506-X Security Appliances ASA 5508-X Security Appliances ASA 5516-X Security Appliances ASA Software, FTD Software, IOS Software, IOS XE Software if they had the DHCPv6 client feature enabled: ASR 1000 Series Aggregation Services Routers Business 150 APs and 151 Mesh Extenders Catalyst 8000 Edge Platforms Family Catalyst 8000V Edge Software Routers Catalyst 8200 Series Edge Platforms Catalyst 8300 Series Edge Platforms Catalyst 8500L Series Edge Platforms Catalyst 9100 APs Catalyst 9200 Series Switches Catalyst 9300 Series Switches Catalyst 9800 Embedded Wireless Controllers for Catalyst 9300, 9400, and 9500 Series Switches Catalyst 9800 Series Wireless Controllers Catalyst 9800-CL Wireless Controllers for Cloud Catalyst IW6300 Heavy Duty Series APs Catalyst IW9165 Heavy Duty Series Catalyst IW9165 Rugged Series Catalyst IW9167 Heavy Duty Series Cisco DNA Center in the default configuration. Cisco DNA Center Software Release 2.3.5 and earlier Cisco IOS XE Software if it had the web UI enabled. Cisco products if they are running Cisco IOS XE Software releases 17.9.1, 17.9.1a, or 17.9.1w and have a tunnel interface configured. Cisco products that are running a vulnerable release of Cisco IOS XE Software, with Cisco IOx application hosting feature configured, and the hosted application is running. Cisco Wireless LAN Controller Software Release version 8.10 and earlier Cloud Services Router 1000V Series Embedded Wireless Controllers on Catalyst Access Points Integrated AP on 1100 Integrated Services Routers
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x?product=Cisco&keyword-=2023%20Mar%2022&last_published=2023%20Mar&sort=-day_sir#~Vulnerabilities

Affected Product	**OpenSSL**
Severity	Low
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-0464)
Description	OpenSSL released security updates addressing a denial of service vulnerability that exists in OpenSSL versions 3.1, 3.0, 1.1.1 and 1.0.2. This security vulnerability has been identified in all supported versions of OpenSSL related to the verification of X.509 certificate chains that include policy constraints. Attackers may be able to exploit this vulnerability by creating a malicious certificate chain that triggers the exponential use of computational resources, leading to a denial-of-service (DoS) attack on affected systems. OpenSSL recommends to apply necessary fixes to avoid issues.
Affected Products	OpenSSL 3.1, 3.0, 1.1.1 and 1.0.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20230322.txt

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.