TLP: WHITE

Advisory Alert

Alert Number: **AAA20230223** **Date:** **February 23, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2020-12930, CVE-2020-12931, CVE-2021-26392, CVE-2021-26393)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Privilege escalation, out-of-bounds write condition and data poisoning. **CVE-2020-12930-** A vulnerability in AMD Secure Processor drivers may allow a privileged attacker to elevate their privileges due to improper parameter handling. **CVE-2020-12931-** A vulnerability in AMD Secure Processor Kernel may allow a privileged attacker to elevate their privileges due to improper parameter handling. **CVE-2021-26392-** A vulnerability in 'LoadModule' may lead to an out-of-bounds write potentially allowing a privileged attacker to gain code execution of the OS/kernel by loading a malicious TA. **CVE-2021-26393-** A vulnerability in AMD Secure Processor Trusted Execution Environment (TEE) may allow a privileged authenticated attacker to generate a valid, signed TA and potentially poison the contents of the process memory with attacker controlled data. Dell recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Dell Aurora R14 Dell Inspiron 3505 Dell Inspiron 3515 Dell Inspiron 3525 Dell Inspiron 3585 Dell Inspiron 3785 Dell Inspiron 5485 Dell Inspiron 5485 2-in-1 Dell Inspiron 5585 Dell Latitude 5495 Dell OptiPlex 5055 Ryzen CPU Dell Vostro 3405 Dell Vostro 3515 Dell Vostro 3525
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000208397/dsa-2023-051

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-20012, CVE-2023-20015, CVE-2023-20050, CVE-2023-20016, CVE-2023-20089, CVE-2023-20011)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to Authentication Bypass, Denial of Service, Command Injection and Cross-Site Request Forgery. Cisco recommends to apply necessary fixes to avoid issues.
Affected Products	Cisco APIC Release 5.2 , 6.0 v Cisco Nexus 9000 Series PIDs when configured in FEX mode Firepower 4100 Series with Cisco FXOS or NX-OS Software Firepower 9300 Security Appliances Cisco FXOS or NX-OS Software MDS 9000 Series Multilayer Switches Nexus 1000 Virtual Edge for VMware vSphere Nexus 1000V Switch for Microsoft Hyper-V Nexus 1000V Switch for VMware vSphere Nexus 3000 and 9000 Series Switches running on NX-OS Software Release 10.2(4) Nexus 3000 and 9000 Series Switches running on NX-OS Software Release 9.3(10) Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 7000 Series Switches running on NX-OS Software Release 8.2(9) UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects Software Release 4.0 UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects Software Release 4.1 UCS 6200, 6300, 6400, and 6500 Series Fabric Interconnects Software Release 4.2 UCS 6200, 6300, 6400, and 6500 Series with Cisco FXOS or NX-OS Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-elyfex-dos-gfvcByx https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxfp-cmdinj-XXBZjtR https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cli-cmdinject-euQVK9u https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucsm-bkpsky-H8FCQgsA https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-lldp-dos-ySCNZOpX https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-capic-csrfv-DMx6KSwV

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.