Advisory Alert

Alert Number: **AAA20230929** **Date:** **September 29, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
HPE	**Critical**	Remote Authentication Bypass Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20034, CVE-2023-20252, CVE-2023-20253,CVE-2023-20254, CVE-2023-20262
Description	Cisco has released security updates addressing multiple critical vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Unauthorized Access, Information Disclosure, Authorization Bypass, Denial of Service. Cisco highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Cisco Catalyst SD-WAN Manager releases 20.9.3, 20.9.1, 20.8.1, 20.7.1, 20.6.3.4, 20.6.2, 20.6.1, 20.3.7, 20.3.4, 20.12.1, 20.11.1, 20.10.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-12900, CVE-2023-28321, CVE-2022-35252, CVE-2022-43552, CVE-2023-27535, CVE-2020-35512, CVE-2022-23990, CVE-2022-3219, CVE-2021-4209, CVE-2020-17049, CVE-2022-36227, CVE-2023-29383, CVE-2019-12904,CVE-2023-28484, CVE-2023-29469, CVE-2021-24032, CVE-2018-1000654, CVE-2019-17543, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-2650, CVE-2022-3204, CVE-2019-16866, CVE-2020-24736, CVE-2019-19244, CVE-2019-9936, CVE-2019-9937, CVE-2023-26604, CVE-2023-24329, CVE-2022-41973, CVE-2020-8911, CVE-2022-2582, GHSA-76wf-9vgp-pj7w, PRISMA-2021-0214, CVE-2018-15919, CVE-2019-6110, CVE-2020-8912, CVE-2019-9923, CVE-2019-11254, CVE-2021-4235, CVE-2023-34969, CVE-2021-42694, CVE-2021-20657, CVE-2019-14250, CVE-2021-39537, CVE-2018-19211, CVE-2018-19217, CVE-2018-20839, CVE-2022-0227, CVE-2021-45985, CVE-2018-20657 , CVE-2018-1000879, CVE-2018-1000880, CVE-2020-21674)
Description	Dell has released security updates addressing multiple critical vulnerabilities that exist in third part products that in turn affect Dell products. Successful exploitation of these vulnerabilities could lead to multiple flaws. Dell highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Dell Container Storage Modules Versions prior to 1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218111/dsa-2023-372-dell-container-storage-modules-security-update-for-multiple-third-party-vulnerabilities

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Remote Authentication Bypass Vulnerabilities (CVE-2023-30908, CVE-2023-30909)
Description	HPE has released security updates addressing multiple critical remote authentication bypass vulnerabilities that exist in HPE OneView Software. HPE highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	HPE OneView all version prior to 6.60.05 HPE OneView 8.10.00 HPE OneView 8.20.00 HPE OneView 8.30.00 HPE OneView 8.40.00 HPE OneView 7.00.00 HPE OneView 7.10.00 HPE OneView 7.20.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04538en_us

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4401, CVE-2023-43068, CVE-2023-43069, CVE-2023-43070, CVE-2023-43071, CVE-2023-43072, CVE-2023-43073, CVE-2022-40982, CVE-2022-43505, CVE-2023-23908, CVE-2022-41804, CVE-2023-20594, CVE-2023-20597)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to multiple flaws. Dell recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	SmartFabric Storage Software Debian package v1.4.1 for upgrading SmartFabric Storage Software VM deployed on either ESXi or linux KVM - v1.4.0 and prior SmartFabric Storage Software package v1.4.1 for ESXi - v1.4.0 and prior SmartFabric Storage Software package v1.4.1 for Linux KVM - v1.4.0 and prior PowerFlex appliance - Intelligent Catalogue (IC) - Versions prior to 45.373.00 PowerFlex rack – RCM - Versions prior to 3.7.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218107/security-update-for-dell-smartfabric-storage-software https://www.dell.com/support/kbdoc/en-us/000218104/dsa-2023-312-security-update-for-dell-powerflex-appliance-multiple-third-party-component-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000218101/dsa-2023-311-security-update-for-dell-powerflex-rack-multiple-thir1d-party-component-vulnerabilities

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20231, CVE-2023-20187, CVE-2023-20227, CVE-2023-20223, CVE-2023-20033, CVE-2023-20226, CVE-2023-20186, CVE-2023-20269, CVE-2023-20202, CVE-2023-20179, CVE-2023-20109, CVE-2023-20176, CVE-2023-20251)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to Authorization Bypass, Command Injection, Denial of Service, Unauthorized Access. Cisco recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-vman-sc-LRLfu2z https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdij-FzZAeXAy https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-mlre-H93FswRz https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-l2tp-dos-eB5tuFmV https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ins-acc-con-nHAVDRBZ https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cat3k-dos-ZZA4Gb3r https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-appqoe-utd-dos-p8O57p5y https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aaascp-Tyj4fEJm https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ravpn-auth-8LyfCkeC https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-wncd-HFGMsfSD https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-html-3ZKh8d6x https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-getvpn-rce-g8qR68sx https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-click-ap-dos-wdcXkvnQ

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.