Advisory Alert

Alert Number: **AAA20230713** **Date:** **July 13, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sonicwall	**Critical**	Multiple Vulnerabilities
Cisco	**Critical**	Unauthenticated REST API Access Vulnerability
Dell	**High**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
F5	**Medium**	Incorrect Permission Assignment Vulnerability
PaloAlto	**Medium**	Information Exposure Vulnerability

Description

Affected Product	**Sonicwall**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34123, CVE-2023-34124, CVE-2023-34125, CVE-2023-34126, CVE-2023-34127, CVE-2023-34128, CVE-2023-34129, CVE-2023-34130, CVE-2023-34131, CVE-2023-34132, CVE-2023-34133, CVE-2023-34134, CVE-2023-34135, CVE-2023-34136, CVE-2023-34137)
Description	Sonicwall has released a security update addressing multiple vulnerabilities within their products. Exploitation of these vulnerabilities leads to exposure of Sensitive Information, Improper Neutralization of Special Elements, Path Traversal, Authentication Bypass. Sonicwall highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	GMS - Virtual Appliance 9.3.2-SP1 and earlier versions GMS - Windows 9.3.2-SP1 and earlier versions Analytics - 2.5.0.4-R7 and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0010

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Unauthenticated REST API Access Vulnerability (CVE-2023-20214)
Description	Cisco has released a security update addressing an Unauthenticated REST API Access vulnerability within REST API of Cisco SD-WAN vManage software. The vulnerability can be exploited by sending a crafted API request to an affected vManage instance. A successful exploit could allow the attacker to retrieve information from and send information to the configuration of the affected Cisco vManage instance. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco SD-WAN vManage Releases 18.3, 20.1, 20.6.3.3, 20.6.4, 20.6.5, 20.7, 20.8, 20.9, 20.11
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-unauthapi-sphCLYPA

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-26343, CVE-2022-32231, CVE-2021-0154, CVE-2021-0153, CVE-2021-33123, CVE-2021-0190, CVE-2021-33122, CVE-2021-0189, CVE-2021-33124, CVE-2021-33103, CVE-2021-0159, CVE-2021-0188, CVE-2021-0155, CVE-2022-34377, CVE-2022-34376, CVE-2022-34406, CVE-2022-34407, CVE-2022-34408, CVE-2022-34409, CVE-2022-34410, CVE-2022-34411, CVE-2022-34412, CVE-2022-34413, CVE-2022-34414, CVE-2022-34415, CVE-2022-34416, CVE-2022-34417, CVE-2022-34418, CVE-2022-34419, CVE-2022-34420, CVE-2022-34421, CVE-2022-34422, CVE-2022-34423, CVE-2022-44640, CVE-2022-0778, CVE-2021-20235, CVE-2021-36299, CVE-2021-21581, CVE-2021-21580, CVE-2021-21579, CVE-2021-21578, CVE-2021-21577, CVE-2021-21576, CVE-2021-36301, CVE-2021-36300, CVE-2022-34435, CVE-2021-3712, CVE-2021-36348, CVE-2021-36347)
Description	Dell has released a security update addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Privilege Escalation, Arbitrary code execution, Content spoofing / Text injection, Denial of service. Dell highly recommends applying necessary fixes to avoid issues.
Affected Products	PowerScale Node Firmware Package Versions prior to 11.7 within • Isilon A200 • Isilon A2000 • PowerScale Archive A300 • PowerScale Archive A3000 • PowerScale B100 • PowerScale F200 • PowerScale F600 • PowerScale F900 • Isilon H400 • PowerScale Hybrid H700 • PowerScale Hybrid H7000 • PowerScale P100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000215747/dsa-2023-205-security-update-for-dell-powerscale-onefs-for-multiple-vulnerabilities

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1077, CVE-2023-1249, CVE-2023-2002, CVE-2023-3090, CVE-2023-3141, CVE-2023-3159, CVE-2023-3161, CVE-2023-3268, CVE-2023-3358, CVE-2023-35788, CVE-2023-35823, CVE-2023-35824, CVE-2023-35828)
Description	Suse has a released security update addressing multiple vulnerabilities affecting their products. Exploitation of the most severe vulnerabilities could lead to Heap out-of-bounds write, Use-after-free flaw, NULL pointer dereference. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP3 SUSE Real Time Module 15-SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20232810-1/

Affected Product	**Ubuntu**
Severity	**High ,Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35788, CVE-2022-29901, CVE-2022-26373, CVE-2023-3111, CVE-2021-20321, CVE-2023-1990, CVE-2021-3753, CVE-2022-1184, CVE-2023-1380, CVE-2023-32233, CVE-2022-4129, CVE-2023-2162, CVE-2023-26545, CVE-2022-3108, CVE-2023-1670, CVE-2023-1998, CVE-2022-3707, CVE-2023-1281, CVE-2023-1118, CVE-2023-30456, CVE-2023-0459, CVE-2023-2985, CVE-2023-1074, CVE-2023-2612, CVE-2023-1859, CVE-2023-32269, CVE-2023-1076, CVE-2022-3903, CVE-2023-1073, CVE-2023-1079, CVE-2023-0458, CVE-2023-1829, CVE-2023-1078, CVE-2023-3161, CVE-2023-25012, CVE-2023-1075, CVE-2023-1513, CVE-2023-1077, CVE-2023-31436, CVE-2023-2124, CVE-2023-2176)
Description	Ubuntu has released security updates addressing Multiple Vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service, Sensitive information disclosure and Arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 20.04 Ubuntu 22.04 Ubuntu 23.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6220-1 https://ubuntu.com/security/notices/USN-6221-1 https://ubuntu.com/security/notices/USN-6222-1 https://ubuntu.com/security/notices/USN-6223-1 https://ubuntu.com/security/notices/USN-6224-1

Affected Product	**F5**
Severity	**Medium**
Affected Vulnerability	Incorrect Permission Assignment Vulnerability (CVE-2023-22326)
Description	F5 has released a patch update to addressing an Incorrect Permission Assignment vulnerability that exists in iControl REST and TMOS shell (tmsh) dig command. The flaw allows an authenticated attacker with resource administrator role privilege to view sensitive information. F5 highly recommends to apply the available patch updates at your earliest to avoid issues.
Affected Products	BIG-IP (all modules) 17.0.0 BIG-IP (all modules) 16.1.0 - 16.1.3 BIG-IP (all modules) 15.1.0 - 15.1.8 BIG-IP (all modules) 14.1.0 - 14.1.5 BIG-IP (all modules) 13.1.0 - 13.1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K83284425

Affected Product	**PaloAlto**
Severity	**Medium**
Affected Vulnerability	Information Exposure Vulnerability (CVE-2023-38046)
Description	PaloAlto has release a security update addressing an Information exposure vulnerability within PAN-OS software. The flaw allows an authenticated administrator with the privilege to commit a specifically created configuration to read local files and resources from the system. PaloAlto recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	PAN-OS 11.0 < 11.0.1 PAN-OS 10.2 < 10.2.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-38046

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.