Advisory Alert

Alert Number: AAA20231017 **Date:** October 17, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Privilege Escalation Vulnerability
SonicWall	**High**	Multiple Vulnerabilities
Dell	**Medium**	Buffer Overflow Vulnerability
IBM	**Medium**	Denial of Service Vulnerability

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-20198)
Description	Cisco has released important security update to address privilege escalation vulnerability in various products. This vulnerability allows a remote, unauthenticated attacker to create an account on an affected system with privilege access. The attacker can then use that account to gain control of the affected system. It is strongly recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Cisco IOS XE Software if the web UI feature is enabled
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-39276, CVE-2023-39277, CVE-2023-39278, CVE-2023-39279, CVE-2023-39280, CVE-2023-41711, CVE-2023-41712, CVE-2023-41713, CVE-2023-41715)
Description	SonicWall has released important security update to address multiple vulnerabilities in various products. The SonicOS Management web interface and SSLVPN portal have been impacted by several vulnerabilities such as Post-authentication Stack-Based Buffer Overflow, Use of Hard-coded Password, Post-authentication Improper Privilege Management vulnerabilities. SonicWall recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	**Gen7** TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 870 - 7.0.1-5119 and older versions **NSsp 15700** 7.0.1-5129 and older versions **Gen6 SonicOSv** NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on VMWare, NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on Hyper-V, NSv (10, 25, 50, 100, 200, 300, 400, 800, 1600) on KVM, NSv (200, 400, 800, 1600) on AWS NSv (200, 400, 800, 1600) on AWS-PAYG, NSv (200, 400, 800, 1600) on Azure, 6.5.4.4-44v-21-2079 and older versions **Gen6 Firewalls** SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W 6.5.4.12-101n and older versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0012

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Buffer Overflow Vulnerability (CVE-2023-32461)
Description	Dell has released a security update to address in Dell PowerEdge BIOS and Dell Precision BIOS contain a buffer overflow vulnerability. A local malicious user with high privileges could potentially exploit this vulnerability, leading to corrupt memory and potentially escalate privileges. Dell recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	PowerEdge R660 Version 1.5.6 or later PowerEdge R760 Version 1.5.6 or later PowerEdge C6620 Version 1.5.6 or later PowerEdge MX760c Version 1.5.6 or later PowerEdge R860 Version 1.5.6 or later PowerEdge R960 Version 1.5.6 or later PowerEdge HS5610 Version 1.5.6 or later PowerEdge HS5620 Version 1.5.6 or later PowerEdge R660xs Version 1.5.6 or later PowerEdge R760xs Version 1.5.6 or later PowerEdge R760xd2 Version 1.5.6 or later PowerEdge T560 Version 1.5.6 or later PowerEdge R760xa Version 1.1.3 or later PowerEdge XE9680 Version 1.1.3 or later PowerEdge XR5610 Version 1.1.4 or later PowerEdge XR8620t Version 1.1.3 or later PowerEdge XR7620 Version 1.5.6 or later PowerEdge XE8640 Version 1.2.5 or later PowerEdge R6615 Version 1.3.11 or later PowerEdge R7615 Version 1.3.11 or later PowerEdge R6625 Version 1.3.11 or later PowerEdge R7625 Version 1.3.11 or later PowerEdge R650 Version 1.10.2 or later PowerEdge R750 Version 1.10.2 or later PowerEdge R750XA Version 1.10.2 or later PowerEdge C6520 Version 1.10.2 or later PowerEdge MX750C Version 1.10.2 or later PowerEdge R550 Version 1.10.2 or later PowerEdge R450 Version 1.10.2 or later PowerEdge R650XS Version 1.10.2 or later PowerEdge R750XS Version 1.10.2 or later PowerEdge T550 Version 1.10.2 or later PowerEdge XR11 Version 1.10.2 or later PowerEdge XR12 Version 1.10.2 or later PowerEdge T150 Version 1.6.3 or later PowerEdge T350 Version 1.6.3 or later PowerEdge R250 Version 1.6.3 or later PowerEdge R350 Version 1.6.3 or later PowerEdge XR4510c Version 1.10.4 or later PowerEdge XR4520c Version 1.10.4 or later PowerEdge R6515 Version 2.11.4 or later PowerEdge R6525 Version 2.11.3 or later PowerEdge R7515 Version 2.11.4 or later PowerEdge R7525 Version 2.11.3 or later PowerEdge C6525 Version 2.11.3 or later PowerEdge XE8545 Version 2.11.3 or later Dell EMC XC Core XC450 Version 1.11.2 or later Dell EMC XC Core XC650 Version 1.11.2 or later Dell EMC XC Core XC750 Version 1.11.2 or later Dell EMC XC Core XC750xa Version 1.11.2 or later Dell EMC XC Core XC6520 Version 1.11.2 or later Dell EMC XC Core XC7525 Version 2.11.3 or later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216543/dsa-2023-292-security-update-for-dell-poweredge-server-bios-vulnerability

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2023-30987)
Description	IBM has released a security update to address in a denial of service vulnerability. IBM Db2 for Linux, UNIX and Windows is vulnerable to denial of service with a specially crafted query on certain databases. IBM recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	IBM Db2 10.5.0.x IBM Db2 11.1.4.x IBM Db2 11.5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7047560

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.