Advisory Alert

Alert Number: AAA20230914 **Date:** September 14, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Palo Alto	**High**, Medium	Multiple Vulnerabilities
Fortinet	**High**, Medium, Low	Multiple Vulnerabilities
Dell	Medium	Improper input validation vulnerability
Cisco	Medium	Multiple Vulnerabilities

Description

Affected Product	**Palo Alto**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3280, CVE-2023-38802)
Description	Palo Alto has released security updates addressing multiple vulnerabilities within their products. If exploited theses vulnerabilities could lead to Denial of service and Improper Handling of Exceptional Conditions. Palo Alto recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cortex XDR Agent 8.0 versions before 8.0.2 on Windows Cortex XDR Agent 7.9-CE versions before 7.9.101-CE on Windows Cortex XDR Agent 7.9 versions before 7.9.3 on Windows Cortex XDR Agent 7.5-CE All versions on Windows Cortex XDR Agent 5.0 All versions on Windows PAN-OS 11.0 versions before 11.0.3 PAN-OS 10.2 versions before 10.2.6 PAN-OS 10.1 versions before 10.1.11 PAN-OS 9.1 , version 9.1.16 and versions before 9.1.16
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2023-3280 https://security.paloaltonetworks.com/CVE-2023-38802

Affected Product	**Fortinet**	
Severity	**High**, Medium, Low	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-35849, CVE-2023-25608, CVE-2023-36634, CVE-2021-44172, CVE-2023-36638, CVE-2023-29183, CVE-2023-27998, CVE-2023-36551, CVE-2023-36642, CVE-2023-40715, CVE-2023-40717, CVE-2023-34984.)	
Description	Fortinet has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead Command injection, Arbitrary file read, Information disclosure, unauthorized code or commands Execution. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.	
Affected Products	FortiADC version 7.1.0 through 7.1.1 FortiADC version 7.0.0 through 7.0.3 FortiADC version 6.2.0 through 6.2.5 FortiADC version 6.1.0 all versions FortiAP-W2 version 7.2.0 through 7.2.1 FortiAP-W2 version 7.0.3 through 7.0.5 FortiAP-W2 version 7.0.0 through 7.0.1 FortiAP-W2 6.4 all versions FortiAP-W2 6.2 all versions FortiAP-W2 6.0 all versions FortiAP-C version 5.4.0 through 5.4.4 FortiAP-C 5.2 all versions FortiAP version 7.2.0 through 7.2.1 FortiAP version 7.0.0 through 7.0.5 FortiAP 6.4 all versions FortiAP 6.0 all versions FortiAP-U version 7.0.0 FortiAP-U version 6.2.0 through 6.2.5 FortiAP-U 6.0 all versions FortiAP-U 5.4 all versions FortiClientEMS version 7.0.6 through 7.0.7 FortiClientEMS version 7.0.0 through 7.0.4 FortiClientEMS 6.4 all versions FortiClientEMS 6.2 all versions	FortiManager version 7.2.0 through 7.2.2 FortiManager version 7.0.0 through 7.0.7 FortiManager version 6.4.0 through 6.4.11 FortiManager 6.2 all versions FortiManager 6.0 all versions FortiAnalyzer version 7.2.0 through 7.2.2 FortiAnalyzer version 7.0.0 through 7.0.7 FortiAnalyzer version 6.4.0 through 6.4.11 FortiAnalyzer 6.2 all versions FortiAnalyzer 6.0 all versions FortiProxy version 7.2.0 through 7.2.4 FortiProxy version 7.0.0 through 7.0.10 FortiOS version 7.2.0 through 7.2.4 FortiOS version 7.0.0 through 7.0.11 FortiOS version 6.4.0 through 6.4.12 FortiOS version 6.2.0 through 6.2.14 FortiPresence version 1.2.0 through 1.2.1 FortiPresence 1.1 all versions FortiPresence 1.0 all versions FortiSIEM version 6.7.0 through 6.7.5 FortiTester 2.3 - 7.2 all versions FortiWeb version 7.2.0 through 7.2.1 FortiWeb version 7.0.0 through 7.0.6 FortiWeb 6.4 all versions FortiWeb 6.3 all versions
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-310 https://www.fortiguard.com/psirt/FG-IR-22-120 https://www.fortiguard.com/psirt/FG-IR-23-123 https://www.fortiguard.com/psirt/FG-IR-21-244 https://www.fortiguard.com/psirt/FG-IR-22-522 https://www.fortiguard.com/psirt/FG-IR-23-106 https://www.fortiguard.com/psirt/FG-IR-22-288 https://www.fortiguard.com/psirt/FG-IR-23-126 https://www.fortiguard.com/psirt/FG-IR-22-501 https://www.fortiguard.com/psirt/FG-IR-22-465 https://www.fortiguard.com/psirt/FG-IR-22-245 https://www.fortiguard.com/psirt/FG-IR-23-068	

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Improper input validation vulnerability(CVE-2021-0135)
Description	Dell has released a security update addressing an Improper input validation vulnerability in Intel Driver affecting Dell Server Update Utility. This vulnerability exists due to insufficient validation of user-supplied input. A local administrator can pass specially crafted input to the application and gain elevated privileges on the target system. Dell recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	Dell Server Update Utility Versions prior to 23.07.00
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000217642/dsa-2023-329-security-update-for-server-update-utility

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20135, CVE-2023-20236, CVE-2023-20233, CVE-2023-20191, CVE-2023-20190)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to arbitrary code execution, Privilege Escalation, Denial of Service. Cisco recommends to apply the necessary security fixes at your earliest to avoid issues
Affected Products	8000 Series Routers With Cisco IOS XR Software 7.7 and later ASR 9000 Series Aggregation Services Routers With Cisco IOS XR Release 7.10 Cisco products with Cisco IOS XR 7.3 , 7.5, 7.8, 7.9 and had a classic IPv4 ACL with either level 2 or level 3 compression applied Cisco Products With Cisco IOS XR Release 7.5 , 7.6, 7.7, 7.8, 7.9 and CFM feature enabled IOS XR White box (IOSXRWBD) with Cisco IOS XR 7.7, 7.9, 7.10 and had MPLS packet filtering enabled NCS 4000 Series With Cisco IOS XR Release 7.10 NCS 5000 Series With Cisco IOS XR Release 7.10 NCS 540 Series Routers With Cisco IOS XR Release 7.10 NCS 5500 Series with Cisco IOS XR 7.7, 7.9 and had MPLS packet filtering NCS 5500 Series With Cisco IOS XR Release 7.10 NCS 560 Series Routers with Cisco IOS XR 7.7, 7.9 and had MPLS packet filtering NCS 560 Series Routers With Cisco IOS XR Release 7.10 NCS 5700 Series with Cisco IOS XR 7.7, 7.9 and had MPLS packet filtering NCS 5700 Series With Cisco IOS XR Release 7.10 Network Convergence Series (NCS) 540 Series Routers with Cisco IOS XR 7.7, 7.9, 7.10 and had MPLS packet filtering Network Convergence System (NCS) 1000 Series With Cisco IOS XR Release 7.10 Network Convergence System (NCS) 540 Series Routers that are running the NCS540L images With Cisco IOS XR Software 7.7 and later Network Convergence System (NCS) 5700 Series Routers that are running the NCS5700 images (NCS-57B1-5DSE-SYS, NCS-57B1-6D24-SYS and NCS-57C1-48Q6-SYS) With Cisco IOS XR Software 7.7 and later
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-lnt-L9zOkBz5 https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-ipxe-sigbypass-pymfyqgB https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xr-cfm-3pWN8MKt https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnx-acl-PyzDkeYF https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-comp3acl-vGmp6BQ3

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.