Advisory Alert

Alert Number: AAA20220812 **Date:** August 12, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PaloAlto	**HIgh**	Denial Of Service Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**PaloAlto**
Severity	**High**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2022-0028)
Description	PaloAlto has released a patch update addressing a Denial-of-service vulnerability that exists because of a flaw in the PAN-OS URL filtering policy misconfiguration. This flaw could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. To carry out this attack, the firewall configuration must have a URL filter profile with one or more blocked categories assigned to a source zone with an external-facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. PaloAlto highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	PAN-OS 10.2 versions earlier than 10.2.2-h2 PAN-OS 10.1 versions earlier than 10.1.6-h6 PAN-OS 10.0 versions earlier than 10.0.11-h1 PAN-OS 9.1 versions earlier than 9.1.14-h4 PAN-OS 9.0 versions earlier than 9.0.16-h3 PAN-OS 8.1 versions earlier than 8.1.23-h1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0028

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1585, CVE-2022-20713, CVE-2022-20866, CVE-2022-20715)
Description	Cisco has released security updates addressing multiple vulnerabilities which may lead attackers to could cause arbitrary code execution on users operating system, conduct browser-based attacks, stealing the RSA private key and cause DOS attacks. **CVE-2021-1585** - The Cisco Adaptive Security Device Manager Launcher could allow an unauthenticated, remote attacker to execute arbitrary code on a user's operating system. This vulnerability is due to a lack of proper signature verification for specific code exchanged between the ASDM and the Launcher. An attacker could exploit this vulnerability by leveraging a man-in-the-middle position on the network to intercept the traffic between the Launcher and the ASDM and then inject arbitrary code **CVE-2022-20713** - The Clientless SSL VPN component of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct browser-based attacks. This vulnerability is due to improper validation of input that is passed to the Clientless SSL VPN component. **CVE-2022-20866** - The handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware based cryptography. **CVE-2022-20715** - The remote access SSL VPN features of Cisco Adaptive Security Appliance Software and Cisco Firepower Threat Defense Software could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Adaptive Security Device Manager 7.18.1.152.and earlier Cisco devices that running on Cisco ASA Software earlier than Release 9.17 with Clientless SSL VPN feature enabled ASA 5506-X with FirePOWER Services ASA 5506H-X with FirePOWER Services ASA 5506W-X with FirePOWER Services ASA 5508-X with FirePOWER Services ASA 5516-X with FirePOWER Services Firepower 1000 Series Next-Generation Firewall Firepower 2100 Series Security Appliances Firepower 4100 Series Security Appliances Firepower 9300 Series Security Appliances Secure Firewall 3100 Cisco products if they are running a vulnerable release of Cisco ASA Software or FTD Software and have a vulnerable AnyConnect or WebVPN configuration
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-webvpn-LOeKsNmO https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rsa-key-leak-Ms7UEfZz https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-tL4uA4AA

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.