Advisory Alert

Alert Number: AAA20220113 **Date:** January 13, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**High**	Multiple vulnerabilities
Cisco	**High**	Multiple vulnerabilities
PaloAlto	**High**	Multiple vulnerabilities

Description

Affected Product	Juniper
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-22152, CVE-2022-22153, CVE-2022-22154, CVE-2022-22155, CVE-2022-22156, CVE-2022-22157, CVE-2022-22167, CVE-2022-22159, CVE-2022-22160, CVE-2022-22161, CVE-2022-22162, CVE-2022-22163, CVE-2022-22164, CVE-2022-22166, CVE-2022-22168, CVE-2022-22169, CVE-2022-22170, CVE-2022-22171, CVE-2022-22172, CVE-2022-22173, CVE-2022-22174, CVE-2022-22175, CVE-2022-22176, CVE-2022-22177, CVE-2022-22178, CVE-2022-22179, CVE-2022-22180, CVE-2019-20372)
Description	Juniper has released security patch updates addressing multiple vulnerabilities that exists in multiple juniper products. An attacker could use these vulnerabilities to gain access to systems and perform malicious activities. Most of the vulnerabilities are found in the Junos OS. It is highly recommended to apply necessary fixes at earliest to the Juniper products to avoid issues.
Affected Products	Multiple Products.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES&cat=SIRT_1&actp=&sort=datemodified&dir=descending&max=1000&batch=15&rss=true&itData.offset=0

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20658, CVE-2022-20652, CVE-2022-20663 CVE-2022-20626, CVE-2022-20656, CVE-2022-20657, CVE-2022-20631, CVE-2022-20632, CVE-2022-20633, CVE-2022-20635, CVE-2022-20636, CVE-2022-20637, CVE-2022-20651)
Description	Cisco has released updates addressing multiple vulnerabilities that exists in their products such as Privilege Escalation Vulnerability, Command Injection Vulnerability, Cross-Site Scripting Vulnerability, Network Manager Vulnerabilities, Information Disclosure Vulnerability. Cisco highly recommends to apply necessary security fixes to avoid issues
Affected Products	Cisco Unified CCMP and Cisco Unified CCDM 11.6.1 and earlier, 12.0.1, 12.5.1, 12.6.1 Cisco Tetration 3.5.1 and earlier, 3.6 Cisco Secure Network Analytics Earlier than 7.2.1 Cisco Prime Access Registrar Appliance 9.2.0.0 and earlier Cisco PI 3.10 Cisco EPNM 5.1.3 Cisco Enterprise Chat and Email Software Earlier than 12.6(1)_ES1 Cisco Security Manager Earlier than 4.24 Cisco Adaptive Security Device Manager Earlier than 7.15.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

Affected Product	PaloAlto
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-0015, CVE-2022-0014, CVE-2022-0012, CVE-2022-0013)
Description	Paloalto has released Security Updates addressing multiple vulnerabilities that exists with Paloalto products. **CVE-2022-0012** - Palo Alto Networks Cortex XDR agent that enables a local user to delete arbitrary system files and impact the system integrity or cause a denial-of-service condition. An improper link resolution before file access vulnerability exists in the Cortex xDR agent on Windows platforms. **CVE-2022-0013** - Information exposure vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables a local attacker to read the contents of arbitrary files on the system with elevated privileges when generating a support file. **CVE-2022-0014** - An untrusted search path vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables a local attacker with file creation privilege in the Windows root directory (such as C:\) to store a program that can then be unintentionally executed by another local user when that user utilizes a Live Terminal session. **CVE-2022-0015** - A local privilege escalation vulnerability exists in the Palo Alto Networks Cortex XDR agent that enables an authenticated local user to execute programs with elevated privileges.
Affected Products	Cortex XDR agent 5.0 versions earlier than Cortex XDR agent 5.0.12 Cortex XDR agent 6.1 versions earlier than Cortex XDR agent 6.1.9 Cortex XDR agent 7.2 versions earlier than Cortex XDR agent 7.2.4 Cortex XDR agent 7.3 versions earlier than Cortex XDR agent 7.3.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2022-0015 https://security.paloaltonetworks.com/CVE-2022-0014 https://security.paloaltonetworks.com/CVE-2022-0012 https://security.paloaltonetworks.com/CVE-2022-0013

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.