Advisory Alert

Alert Number: AAA20211014 **Date:** October 14, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PaloAlto	**High**	Multiple Vulnerabilities
Juniper	**High**	Multiple Vulnerabilities

Description

Affected Product	**PaloAlto**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3057, CVE-2020-1968)
Description	Paloalto has released Security Updates addressing multiple vulnerabilities that exists with Paloalto products. **CVE-2021-3057** - The Palo Alto Networks GlobalProtect app contains a stack-based buffer overflow vulnerability that allows a man in the-middle attacker to disrupt system operations and potentially execute arbitrary code with system privileges. **CVE-2020-1968** - The DHE cipher offered for use in traffic decryption in versions of Palo Alto Networks PAN-OS software prior to PAN-OS 10.0 improperly distributes a cryptographic secret over several TLS connections, weakening its cryptographic strength. This is required for the Raccoon attack (CVE-2020-1968), which allows an attacker to eavesdrop on encrypted communication via TLS connections.
Affected Products	GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.9 on Windows; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.8 on Windows; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.8 on the Universal Windows Platform; GlobalProtect app 5.3 versions earlier than GlobalProtect app 5.3.1 on Linux. PAN-OS 8.1, all versions of PAN-OS 9.0, and all versions of PAN-OS 9.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3057 https://security.paloaltonetworks.com/CVE-2020-1968

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-0296, CVE-2021-0297, CVE-2021-0298, CVE-2021-0299, CVE-2021-31350, CVE-2021-31351, CVE-2021-31352, CVE-2021-31353, CVE-2021-31354, CVE-2021-31355, CVE-2021-31356, CVE-2021-31357, CVE-2021-31358, CVE-2021-31359, CVE-2021-31360, CVE-2021-31361, CVE-2021-31362, CVE-2021-31363, CVE-2021-31364, CVE-2021-31365, CVE-2021-31366, CVE-2021-31367, CVE-2021-31368, CVE-2021-31369, CVE-2021-31370, CVE-2020-27218, CVE-2020-27223, CVE-2021-28165, CVE-2021-22901, CVE-2020-1971, CVE-2021-31371, CVE-2021-31372, CVE-2021-31373, CVE-2021-31374, CVE-2021-31375, CVE-2021-31376, CVE-2021-31377, CVE-2017-13716, CVE-2018-1000654, CVE-2018-7738, CVE-2019-15605, CVE-2019-15606, CVE-2019-18276, CVE-2019-9511, CVE-2019-9513, CVE-2019-9514, CVE-2020-10878, CVE-2020-1971, CVE-2020-7212, CVE-2020-7769, CVE-2020-7788, CVE-2020-8174, CVE-2020-8265, CVE-2004-2320, CVE-2020-25659, CVE-2021-31378, CVE-2021-31379, CVE-2021-31380, CVE-2021-31381, CVE-2021-31382, CVE-2021-31383, CVE-2021-31384, CVE-2021-31385, CVE-2021-31386, CVE-2020-25681, CVE-2020-25682, CVE-2020-25683, CVE-2020-25684, CVE-2020-25685, CVE-2020-25686, CVE-2020-25687, CVE-2021-31349)
Description	Juniper Networks has released Security Updates addressing multiple vulnerabilities that exist with various Juniper products such as Denial of Service (DoS) Vulnerability, Cookie-hijacking Vulnerability, Command Injection Vulnerability, Privilege Escalation Vulnerability, Remote Code Execution Vulnerability, Cross-Site Scripting (XSS) vulnerability, Information Disclosure Vulnerability, Path Traversal Vulnerability, and Authentication Bypass Vulnerability. It is highly recommended to apply the necessary fixes provided on the official Juniper website at the earliest to avoid these security issues. All Juniper users are encouraged to upgrade to the latest versions.
Affected Products	Juniper Networks CTPView Juniper Networks Junos OS Juniper Networks SRC Series Juniper Networks SBR Carrier Juniper Secure Connect Application Juniper Networks Contrail Insights Juniper Networks NorthStar Controller Juniper Networks Contrail Service Orchestration (CSO) Juniper Networks 128 Technology Session Smart Router
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&channel=SECURITY_ADVISORIES

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.