Advisory Alert

Alert Number: AAA20210812 **Date:** August 12, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PaloAlto	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	PaloAlto
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-3050, CVE-2021-3046, CVE-2021-3048, CVE-2021-3045, CVE-2021-3047)
Description	**CVE-2021-3050 -** An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to execute arbitrary OS commands to escalate privileges. **CVE-2021-3046 -** An improper authentication vulnerability exists in Palo Alto Networks PAN-OS software that enables a SAML authenticated attacker to impersonate any other user in the GlobalProtect Portal and GlobalProtect Gateway when they are configured to use SAML authentication. **CVE-2021-3048 -** Certain invalid URL entries contained in an External Dynamic List (EDL) cause the Device Server daemon (devsrvr) to stop responding.This condition causes subsequent commits on the firewall to fail and prevents administrators from performing commits and configuration changes even though the firewall remains otherwise functional. If the firewall then restarts, it results in a denial-of-service (DoS) condition and the firewall stops processing traffic. **CVE-2021-3045 -** The risk of injecting OS command into the Palo Alto Networks Pan-OS web interface allows an authenticated administrator to read an arbitrary file from the file system **CVE-2021-3047 -** Palo Alto Networks uses a symbolically weak pseudo-random number generator (PRNG) for authentication for the Pan-OS web interface. This enables an authenticated attacker, with the capability to observe their own authentication secrets over a long duration on the PAN-OS appliance, to impersonate another authenticated web interface administrator's session.
Affected Products	PAN-OS 9.0 version 9.0.10 through PAN-OS 9.0.14. PAN-OS 9.1 version 9.1.4 through PAN-OS 9.1.10. PAN-OS 10.0 version 10.0.7 and earlier PAN-OS 10.0 versions. PAN-OS 10.1 version 10.1.0 through PAN-OS 10.1.1. PAN-OS 8.1 versions earlier than PAN-OS 8.1.19; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. PAN-OS 9.1 versions earlier than PAN-OS 9.1.10. PAN-OS 9.1 versions earlier than PAN-OS 9.1.10; PAN-OS 10.0 versions earlier than PAN-OS 10.0.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3050 https://security.paloaltonetworks.com/CVE-2021-3046 https://security.paloaltonetworks.com/CVE-2021-3048 https://security.paloaltonetworks.com/CVE-2021-3045 https://security.paloaltonetworks.com/CVE-2021-3047

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.