Advisory Alert

Alert Number : AAA20200910 **Date :** September 10, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Paloalto	**High**	Multiple Vulnerabilities

Description

Affected Product	Paloalto
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-2042), (CVE-2020-2038), (CVE-2020-2041), (CVE-2020-2036)
Description	Paloalto has released security updates to address multiple vulnerabilities in Paloalto products including Buffer overflow vulnerability, command injection vulnerabilities, denial-of-service attack and a reflected cross site scripting vulnerability in management web interface. **CVE-2020-2042**: A buffer overflow vulnerability in the PAN-OS management web interface allows authenticated administrators to disrupt system processes and potentially execute arbitrary code with root privileges. **CVE-2020-2038**: An OS Command Injection vulnerability in the PAN-OS management interface allows authenticated administrative users to execute arbitrary OS commands with root privileges. **CVE-2020-2041**: Insecure configuration of the appweb daemon of Palo Alto networks PAN- OS 8.1 allows unauthenticated remote user to send specifically crafted request to the device that will cause the appweb to crash. **CVE-2020-2036**: An attacker can convince an administrator with an active authenticated session on the firewall management interface to click on a crafted link to a web interface which could execute arbitrary JavaScript code in the administrator's browser and then perform administrative functions.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2020-2042 https://security.paloaltonetworks.com/CVE-2020-2038 https://security.paloaltonetworks.com/CVE-2020-2041 https://security.paloaltonetworks.com/CVE-2020-2036

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.