Palo Alto Networks firewalls remote root code execution Bug

14 Dec 2017

Description

This is a public advisory for CVE-2017-15944 which is a remote root code Execution bug found in Palo Alto Networks firewalls.

Three separate bugs can be used together to remotely execute commands as root through the web management interface without authentication on: PAN-OS 6.1.18 and earlier, PAN-OS 7.0.18 and earlier, PAN-OS 7.1.13 and earlier, PAN-OS 8.0.5 and earlier.

Palo Alto Networks recommends not exposing the web management interface to the internet.

Severity: Critical

Bugs:

Bug #1: Partial authentication bypass
Bug #2: Arbitrary directory creation
Bug #3: Command injection in cron script

Products Affected:

PAN-OS 6.1.18 and earlier, PAN-OS 7.0.18 and earlier, PAN-OS 7.1.13 and earlier, PAN-OS 8.0.5 and earlier.

Available Updates:

PAN-OS 6.1.19 and later, PAN-OS 7.0.19 and later, PAN-OS 7.1.14 and later, PAN-OS 8.0.6 and later

Reference Link:

https://securityadvisories.paloaltonetworks.com/Home/Detail/102?AspxAutoDetectCookieSupport=1

http://seclists.org/fulldisclosure/2017/Dec/38

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15944