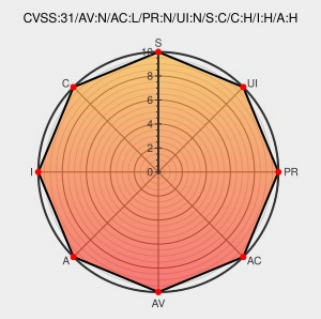
CVE-2019-17440

Published on: 12/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:37 PM UTC

CVE-2019-17440 - advisory for PAN-SA-2019-0040

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Pa-7050 from Paloaltonetworks contain the following vulnerability:

Improper restriction of communications to Log Forwarding Card (LFC) on PA-7000 Series devices with second-generation Switch Management Card (SMC) may allow an attacker with network access to the LFC to gain root access to PAN-OS. This issue affects PAN-OS 9.0 versions prior to 9.0.5-h3 on PA-7080 and PA-7050 devices with an LFC installed and configured. This issue does not affect PA-7000 Series deployments using the first-generation SMC and the Log Processing Card (LPC). This issue does not affect any other PA series devices. This issue does not affect devices without an LFC. This issue does not affect PAN-OS 8.1 or prior releases. This issue only affected a very limited number of customers and we undertook individual outreach to help them upgrade. At the time of publication, all identified customers have upgraded SW or content and are not impacted.

CVE-2019-17440 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as CRITICAL severity.

Palo Alto Networks is not aware of any exploitation of this issue.

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **< 9.0.5-h3**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **! 8.0**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **! 8.1**

Affected Vendor/Software: **Palo Alto Networks** - **PAN-OS** version **!>= 9.0.6, 9.0.5-h3**

Vulnerability Patch/Work Around

(1) Content update 8218-5815 can be applied without requiring a software update. Once the content update is installed please ensure that next PAN-OS upgrade is to a fixed version (9.0.5-h3 or later). Do not upgrade or downgrade to an affected release, as it can reintroduce the vulnerability. (2) Configure security policies to prevent network sessions destined to LFC. (3) Ensure that LFC is only connected to a secured administrative network with access restricted to trusted users. (4) Disable or disconnect LFC from the network until fixes can be applied.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2019-17440 PAN-OS on PA-7000 Series: Improper restriction of communication to Log Forwarding Card (LFC) allows root access	security.paloaltonetworks.com text/html	CONFIRM security.paloaltonetworks.com/CVE-2019-17440

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Paloaltonetworks	Pa-7050	-	All	All	All
Hardware	Paloaltonetworks	Pa-7050	-	All	All	All
Hardware	Paloaltonetworks	Pa-7080	-	All	All	All
Hardware	Paloaltonetworks	Pa-7080	-	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

cpe:2.3:h:paloaltonetworks:pa-7050:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7050:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7080:-:*:*:*:*:*:*:*:

cpe:2.3:h:paloaltonetworks:pa-7080:-:*:*:*:*:*:*:*:

cpe:2.3:o:paloaltonetworks:pan-os:*:*:*:*:*:*:*:*:

Discovery Credit

Palo Alto Networks would like to thank Ayad (Ed) Sleiman, Head of Information Security at King Abdullah University of Science and Technology (KAUST) and his team for discovering and responsibly reporting this issue.

← Previous ID

Next ID→