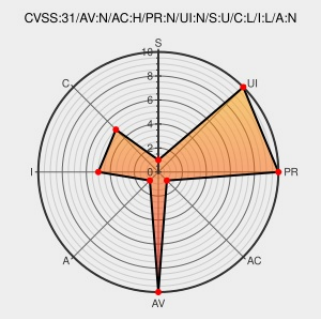
CVE-2020-1982

Published on: 07/08/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:46 PM UTC

CVE-2020-1982

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



Certain versions of Pan-os from Paloaltonetworks contain the following vulnerability:

Certain communication between PAN-OS and cloud-delivered services inadvertently use TLS 1.0, which is known to be a cryptographically weak protocol. These cloud services include Cortex Data Lake, the Customer Support Portal, and the Prisma Access infrastructure. Conditions required for exploitation of known TLS 1.0 weaknesses do not exist for the communication between PAN-OS and cloud-delivered services. We do not believe that any communication is impacted as a result of known attacks against TLS 1.0. This issue impacts: All versions of PAN-OS 8.0; PAN-OS 8.1 versions earlier than PAN-OS 8.1.14; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9; PAN-OS 9.1 versions earlier than PAN-OS 9.1.3. PAN-OS 7.1 is not impacted by this issue.

CVE-2020-1982 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as MEDIUM severity.

Conditions required for exploitation of known TLS 1.0 weaknesses do not exist for the communication between PAN-OS and cloud delivered services. Palo Alto Networks is not aware of any malicious exploitation of this issue.

Vulnerability Patch/Work Around

Since TLS 1.0 weaknesses are exploited by the man-in-the-middle type of attackers, ensuring security of the networks reduces risks of exploitation of these issues.

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
CVE-2020-1982 PAN-OS: TLS 1.0 usage for certain communications with Palo Alto Networks cloud delivered services	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-1982

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All

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

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

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

Discovery Credit

This issue was found by a customer.

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report