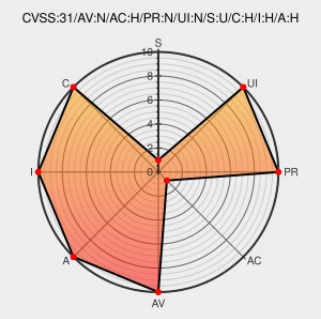
CVE-2020-2002

Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:07 PM UTC

CVE-2020-2002

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



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

An authentication bypass by spoofing vulnerability exists in the authentication daemon and User-ID components of Palo Alto Networks PAN-OS by failing to verify the integrity of the Kerberos key distribution center (KDC) before authenticating users. This affects all forms of authentication that use a Kerberos authentication profile. A man-in-the-middle type of attacker with the ability to intercept communication between PAN-OS and KDC can login to PAN-OS as an administrator. This issue affects: PAN-OS 7.1 versions earlier than 7.1.26; PAN-OS 8.1 versions earlier than 8.1.13; PAN-OS 9.0 versions earlier than 9.0.6; All version of PAN-OS 8.0.

CVE-2020-2002 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Vulnerability Patch/Work Around

Ensure that PAN-OS communicates to Kerberos server over a secured network with access restricted to trusted users. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at: https://docs.paloaltonetworks.com.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
CVE-2020-2002 PAN-OS: Spoofed Kerberos key distribution center authentication bypass	Vendor Advisory security.paloaltonetworks.com text/html	MISC security.paloaltonetworks.com/CVE-2020-2002

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

Palo Alto Networks would like to thank Yoav Iellin, Yaron Kassner, and Rotem Zach from Silverfort for discovering and reporting this issue.

← Previous ID

Next ID→

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