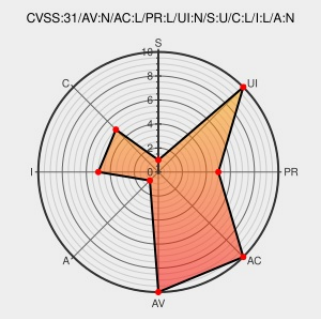
# CVE-2020-1998

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

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

## CVE-2020-1998

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




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

An improper authorization vulnerability in PAN-OS that mistakenly uses the permissions of local linux users instead of the intended SAML permissions of the account when the username is shared for the purposes of SSO authentication. This can result in authentication bypass and unintended resource access for the user. 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; PAN-OS 9.1 versions earlier than 9.1.1; All versions of PAN-OS 8.0.

CVE-2020-1998 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

### Vulnerability Patch/Work Around

The impact of this vulnerability can be mitigated by removing shared usernames between local linux users and SAML enabled users.

### CVSS3 Score: 8.8 - HIGH

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

### CVSS2 Score: 6.5 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| NETWORK | LOW | SINGLE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |

PARTIAL | PARTIAL | PARTIAL

## CVE References

| Description | Tags | Link |
|---|---|---|
| CVE-2020-1998 PAN-OS: Improper SAML SSO authorization of shared local users | Vendor Advisory<br>security.paloaltonetworks.com<br>text/html | MISC<br>security.paloaltonetworks.com/CVE-2020-1998 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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 Maurice Lok-Hin for discovering and reporting this issue.

← Previous ID

Next ID→