**Palo Alto Networks PAN-OS 10.1.x < 10.1.11 / 10.2.x < 10.2.5 / 11.0.x < 11.0.3 Vulnerability**

**HIGH**Nessus Plugin ID 193147

Language:

English

* [Information](https://www.tenable.com/plugins/nessus/193147)
* [Dependencies](https://www.tenable.com/plugins/nessus/193147/dependencies)
* [Dependents](https://www.tenable.com/plugins/nessus/193147/dependents)
* [Changelog](https://www.tenable.com/plugins/nessus/193147/changelog)

**Synopsis**

The remote PAN-OS host is affected by a vulnerability

**Description**

The version of Palo Alto Networks PAN-OS running on the remote host is 10.1.x prior to 10.1.11 or 10.2.x prior to 10.2.5 or 11.0.x prior to 11.0.3. It is, therefore, affected by a vulnerability.  
  
- A vulnerability in how Palo Alto Networks PAN-OS software processes data received from Cloud Identity Engine (CIE) agents enables modification of User-ID groups. This impacts user access to network resources where users may be inappropriately denied or allowed access to resources based on your existing Security Policy rules. (CVE-2024-3383)  
  
Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.

**Solution**

Upgrade to PAN-OS 10.1.11 / 10.2.5 / 11.0.3 or later

**See Also**

<https://security.paloaltonetworks.com/CVE-2024-3383>

**Plugin Details**

**Severity:**High

**ID:**193147

**File Name:**palo\_alto\_CVE-2024-3383.nasl

**Version:**1.2

**Type:**combined

**Family:**[Palo Alto Local Security Checks](https://www.tenable.com/plugins/nessus/families/Palo%20Alto%20Local%20Security%20Checks)

**Published:**4/10/2024

**Updated:**4/11/2024

**Configuration:**Enable paranoid mode

**Supported Sensors:**Nessus

**Risk Information**

[**VPR**](https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss)

**Risk Factor:**Medium

**Score:**6.0

[**CVSS v2**](https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator?vector=AV:N/AC:L/Au:S/C:P/I:P/A:N)

**Risk Factor:**Medium

**Base Score:**5.5

**Temporal Score:**4.1

**Vector:**CVSS2#AV:N/AC:L/Au:S/C:P/I:P/A:N

**CVSS Score Source:**[CVE-2024-3383](https://www.tenable.com/cve/CVE-2024-3383)

[**CVSS v3**](https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C&version=3.0)

**Risk Factor:**High

**Base Score:**7.4

**Temporal Score:**6.4

**Vector:**CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H

**Temporal Vector:**CVSS:3.0/E:U/RL:O/RC:C

**Vulnerability Information**

**CPE:**cpe:/o:paloaltonetworks:pan-os

**Required KB Items:**Host/Palo\_Alto/Firewall/Version, Host/Palo\_Alto/Firewall/Full\_Version, Host/Palo\_Alto/Firewall/Source, Settings/ParanoidReport

**Exploit Ease:**No known exploits are available

**Patch Publication Date:**4/10/2024

**Vulnerability Publication Date:**4/10/2024

**Reference Information**

**CVE:**[CVE-2024-3383](https://www.tenable.com/cve/CVE-2024-3383)

**CWE:**[282](http://cwe.mitre.org/data/definitions/282)

**IAVA:**2024-A-0171