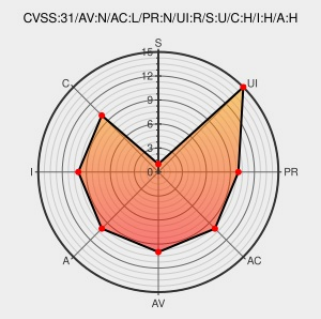
# CVE-2020-2036

Published on: 09/09/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

## CVE-2020-2036

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




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

A reflected cross-site scripting (XSS) vulnerability exists in the PAN-OS management web interface. A remote attacker able to convince an administrator with an active authenticated session on the firewall management interface to click on a crafted link to that management web interface could potentially execute arbitrary JavaScript code in the administrator's browser and perform administrative actions. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.16; PAN-OS 9.0 versions earlier than PAN-OS 9.0.9.

CVE-2020-2036 has been assigned by psirt@paloaltonetworks.com to track the vulnerability - currently rated as HIGH severity.

Palo Alto Networks is not aware of any malicious attempts to exploit this vulnerability.

### Vulnerability Patch/Work Around

Administrators should use caution when they are authenticated to the firewall management web interface and not click or open links from unsolicited sources. This issue impacts the management web interface of PAN-OS. You can mitigate the impact of this issue by following best practices for securing the PAN-OS management web interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at https://docs.paloaltonetworks.com/best-practices.

### CVSS3 Score: 8.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | REQUIRED |
| **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-2020-2036 PAN-OS: Reflected Cross-Site Scripting (XSS) vulnerability in management web interface | Vendor Advisory<br>security.paloaltonetworks.com<br>text/html | CONFIRM<br>security.paloaltonetworks.com/CVE-2020-2036 |



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 |

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

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

## Discovery Credit

Palo Alto Networks thanks Mikhail Klyuchnikov and Nikita Abramov of Positive Technologies and Ben Nott of Palo Alto Networks for discovering and reporting this issue.

← Previous ID

Next ID→