



# CVE-2017-9459

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                          |
|------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2017-9459                                                                                                            |
| <b>State</b>           | PUBLIC                                                                                                                   |
| <b>Assigner</b>        | cve@mitre.org                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                             |
| <b>Published</b>       | 2017-08-02 19:29:00 UTC                                                                                                  |
| <b>Updated</b>         | 2020-02-17 16:15:00 UTC                                                                                                  |
| <b>Description</b>     | Cross-site scripting (XSS) vulnerability in the management web interface in Palo Alto Networks PAN-OS before 6.1.18, 7.x |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

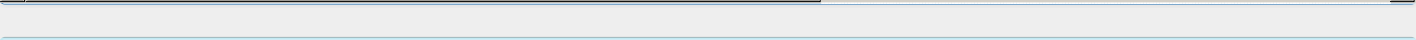
| Type             | Vendor                           | Product                | Version | Update | Edition | Language |
|------------------|----------------------------------|------------------------|---------|--------|---------|----------|
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.1   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.10  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.11  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.12  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.13  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.14  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.15  | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.2   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.3   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.4   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.5   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.6   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.7   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.8   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.0.9   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.0   | All    | All     | All      |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.1   | All    | All     | All      |

[illegible]

|                  |                                  |                        |          |     |     |     |
|------------------|----------------------------------|------------------------|----------|-----|-----|-----|
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.6    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.7    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.8    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.9    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 7.1.9-h2 | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 8.0.0    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 8.0.1    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | 8.0.2    | All | All | All |
| Operating System | <a href="#">Paloaltonetworks</a> | <a href="#">Pan-os</a> | All      | All | All | All |

References

| Reference                                                                                                                                  |
|--------------------------------------------------------------------------------------------------------------------------------------------|
| Palo Alto PAN-OS Input Validation Flaw in Management Web Interface Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTrails |
| Palo Alto Networks PAN-OS CVE-2017-9459 HTML Injection Vulnerability                                                                       |
| CVE-2017-9459 Cross-Site Scripting in the Management Web Interface                                                                         |
| CVE Program record                                                                                                                         |
| NVD vulnerability detail                                                                                                                   |



No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.