



# CVE-2018-7636

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

## Summary

<b>CVE</b>	CVE-2018-7636
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-07-03 21:29:00 UTC
<b>Updated</b>	2020-02-17 16:15:00 UTC
<b>Description</b>	The URL filtering "continue page" hosted by PAN-OS 8.0.10 and earlier may allow an attacker to inject arbitrary JavaScript

## 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>	8.0.10	All	All	All
Operating System	<a href="#">Paloaltonetworks</a>	<a href="#">Pan-os</a>	8.0.10	All	All	All

## References

### Reference

[CVE-2018-7636 Cross Site Scripting in PAN-OS](#)

[Palo Alto Networks PAN-OS CVE-2018-7636 Cross Site Scripting Vulnerability](#)

[Palo Alto PAN-OS Input Validation Flaw in URL Filtering 'continue page' Lets Remote Users Conduct Cross-Site Scripting Attacks - SecurityTr](#)

[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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)