

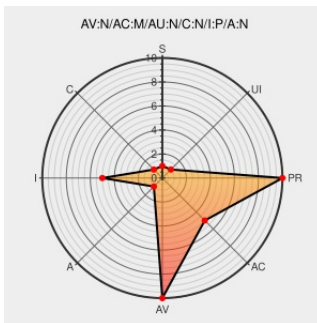


CVE-2014-3764

Published on: 01/06/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:45 PM UTC

CVE-2014-3764

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Pan-os](#) from [Paloaltonetworks](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the web-based device management interface in Palo Alto Networks PAN-OS before 5.0.15, 5.1.x before 5.1.10, and 6.0.x before 6.0.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Ref ID 64563.

CVE-2014-3764 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Security Advisory SA61811 - Palo Alto Networks PAN-OS Cross-Site Scripting Vulnerability - Secunia	web.archive.org text/html	SECUNIA 61811
CVE-2014-3764 Cross-site scripting vulnerability	security.paloaltonetworks.com text/html	CONFIRM security.paloaltonetworks.com/CVE-2014-3764

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 CIDs associated with this CVE

There are currently no CVEs associated with this CPE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Paloaltonetworks	Pan-os	5.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.4	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.6	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.7	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.8	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.9	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.4	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.4	All	All	All

Operating System	Paloaltonetworks	Pan-os	5.1.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.6	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.7	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.8	All	All	All
Operating System	Paloaltonetworks	Pan-os	5.1.9	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.1	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.2	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.3	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.4	All	All	All
Operating System	Paloaltonetworks	Pan-os	6.0.5	All	All	All
Operating System	Paloaltonetworks	Pan-os	All	All	All	All
cpe:2.3:o:paloaltonetworks:pan-os:5.1:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.1:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.2:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.3:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.4:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.5:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.6:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.7:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.8:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:5.1.9:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:6.0:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:6.0.1:*:*:*:*:*:						
cpe:2.3:o:paloaltonetworks:pan-os:6.0.2:*:*:*:*:*:						

cpe:2.3:o:paloaltonetworks:pan-os:6.0.3:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.4:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.5:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.1:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.2:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.3:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.4:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.5:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.6:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.7:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.8:*****:
cpe:2.3:o:paloaltonetworks:pan-os:5.1.9:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.1:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.2:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.3:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.4:*****:
cpe:2.3:o:paloaltonetworks:pan-os:6.0.5:*****:
cpe:2.3:o:paloaltonetworks:pan-os:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)