



CVE-2017-15943

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

Summary

CVE	CVE-2017-15943
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-11 17:29:00 UTC
Updated	2020-02-17 16:15:00 UTC
Description	The configuration file import for applications, spyware and vulnerability objects functionality in the web interface in Palo Alto

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
CVE-2017-15943 Server-Side Request Forgery in PAN-OS	CONFIRM
Palo Alto Networks PAN-OS CVE-2017-15943 Server Side Request Forgery Security Bypass Vulnerability	BID
Palo Alto PAN-OS Access Control Flaw Lets Remote Users Conduct Server-Side Request Forgery Attacks - SecurityTracker	SECTrack
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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