

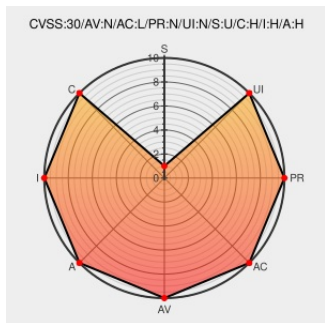


CVE-2017-15944

Published on: 12/11/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:32 PM UTC

CVE-2017-15944

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

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

Palo Alto Networks PAN-OS before 6.1.19, 7.0.x before 7.0.19, 7.1.x before 7.1.14, and 8.0.x before 8.0.6 allows remote attackers to execute arbitrary code via vectors involving the management interface.

CVE-2017-15944 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Palo Alto Networks Firewalls - Root Remote Code Execution	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 43342

Palo Alto PAN-OS Multiple Management Interface Bugs Let Remote Users Execute Arbitrary Commands on the Target System with Root Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTRAK 1040007
CVE-2017-15944 Vulnerability in PAN-OS and Panorama on Management Interface	security.paloaltonetworks.com text/html	 CONFIRM security.paloaltonetworks.com/CVE-2017-15944
Palo Alto Networks - 'readSessionVarsFromFile()' Session Corruption (Metasploit) - Unix remote Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 44597
Palo Alto Networks PAN-OS CVE-2017-15944 Remote Code Execution Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 102079

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 QIDs associated with this CVE

Exploit/POC from Github

Detecion for the vulnerability CVE-2017-15944

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:*****:*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @NIKSUN	The DHS's CISA has added seven new vulnerabilities (CVE-2017-15944, CVE-2022-21971, CVE-2022-26923, CVE-2022-2856,... twitter.com/i/web/status/1...	2022-08-22 13:38:16
 @rnbteam_llc	CVE-2017-15944 CVE-2022-21971 CVE-2022-26923 CVE-2022-2856 CVE-2022-32893 CVE-2022-32894 CVE-2022-22536... twitter.com/i/web/status/1...	2022-08-22 16:55:22

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

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