

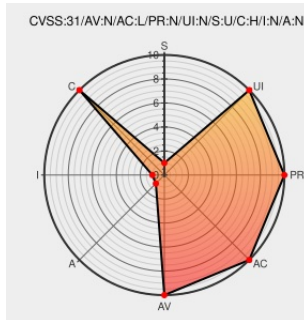


CVE-2020-2012

Published on: 05/13/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:09 PM UTC

CVE-2020-2012

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

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

Improper restriction of XML external entity reference ('XXE') vulnerability in Palo Alto Networks Panorama management service allows remote unauthenticated attackers with network access to the Panorama management interface to read arbitrary files on the system.

This issue affects: All versions of PAN-OS for Panorama 7.1 and 8.0; PAN-OS for Panorama 8.1 versions earlier than 8.1.13; PAN-OS for Panorama 9.0 versions earlier than 9.0.7.

CVE-2020-2012 has been assigned by [psirt@paloaltonetworks.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Vulnerability Patch/Work Around

This issue affects the management interface of PAN-OS and is strongly mitigated by following best practices for securing the PAN-OS management interface. Please review the Best Practices for Securing Administrative Access in the PAN-OS technical documentation, available at: <https://docs.paloaltonetworks.com>

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

PARTIAL

NONE

NONE

CVE References

Description

Tags

Link

CVE-2020-2012 PAN-OS: Panorama: XML external entity reference ('XXE') vulnerability leads the to information leak

Vendor Advisory

security.paloaltonetworks.com

text/html

MISC

security.paloaltonetworks.com/CVE-2020-2012

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

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
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:*****:.*:.*						
cpe:2.3:o:paloaltonetworks:pan-os:*****:.*:.*						
cpe:2.3:o:paloaltonetworks:pan-os:*****:.*:.*						

Discovery Credit

This issue was found by Ben Nott of Palo Alto Networks during internal security review.

[← Previous ID](#)[Next ID →](#)© 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](#).

