



CVE-2020-1977

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

Summary

CVE	CVE-2020-1977
State	PUBLIC
Assigner	psirt@paloaltonetworks.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-12 23:15:00 UTC
Updated	2021-12-30 22:06:00 UTC
Description	Insufficient Cross-Site Request Forgery (XSRF) protection on Expedition Migration Tool allows remote unauthenticated atta

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Paloaltonetworks	Expedition Migration Tool	All	All	All	All

References

Reference	Source	Link
CVE-2020-1977 Expedition Migration Tool: Insufficient Cross Site Request Forgery protection.	CONFIRM	security.paloaltonetworks.com
Palo Alto Expedition Migration Tool Insufficient XSRF Protection - Research Advisory Tenable®	MISC	www.tenable.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Palo Alto Networks thanks Jimi Sebree of Tenable Research for discovering and responsibly reporting this issue.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#)