



CVE-2019-12210

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2019-12210
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-04 21:29:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	In Yubico pam-u2f 1.0.7, when configured with debug and a custom debug log file is set using debug_file, that file descripto

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yubico	Pam-u2f	1.0.7	All	All	All
Application	Yubico	Pam-u2f	1.0.7	All	All	All

References

Reference

[security-announce] openSUSE-SU-2019:1708-1: moderate: Security update f

Do not leak file descriptor when doing exec · Yubico/pam-u2f@18b1914 · GitHub

[security-announce] openSUSE-SU-2019:1725-1: moderate: Security update f

oss-security - pam-u2f: CVE-2019-12210: debug_file file descriptor leak, CVE-2019-12209: symlink attack on u2f_keys leading to possible info

Release Notes

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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](#)