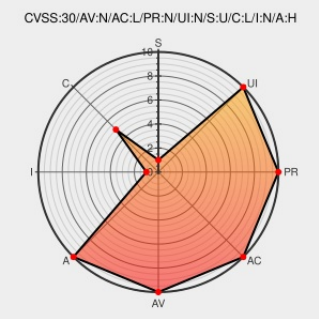
CVE-2018-9275

Published on: 04/04/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:54 PM UTC

CVE-2018-9275

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Yubico Pam from Yubico contain the following vulnerability:

In check_user_token in util.c in the Yubico PAM module (aka pam_yubico) 2.18 through 2.25, successful logins can leak file descriptors to the auth mapping file, which can lead to information disclosure (serial number of a device) and/or DoS (reaching the maximum number of file descriptors).

CVE-2018-9275 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.2 - HIGH

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

CVSS2 Score: 6.4 - MEDIUM

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

CVE References

Description	Tags	Link
Bug 1088027 – VUL-0: CVE-2018-9275: pam_yubico: Authfile Leaking File Descriptor	Issue Tracking, Third Party Advisory, bugzilla.opensuse.org	CONFIRM bugzilla.opensuse.org/show_bug.cgi?id=1088027

	text/html	
util: make sure to close the authfile before returning success · Yubico/yubico-pam@0f6ceab · GitHub	Patch github.com text/html	CONFIRM github.com/Yubico/yubico-pam/commit/0f6ceabab0a8849b47f67d727aa526c2656089ba
Authfile Leaking File Descriptor · Issue #136 · Yubico/yubico-pam · GitHub	Issue Tracking Third Party Advisory github.com text/html	CONFIRM github.com/Yubico/yubico-pam/issues/136

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yubico	Yubico Pam	All	All	All	All

cpe:2.3:a:yubico:yubico_pam:*:*:*:*:*:yubico:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→