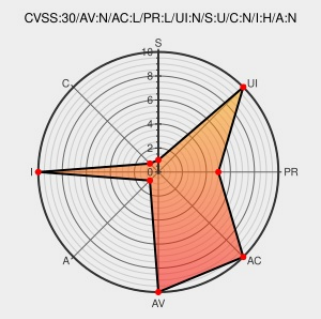
CVE-2018-6558

Published on: 08/23/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:46 PM UTC

CVE-2018-6558

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



Certain versions of Fscrypt from Google contain the following vulnerability:

The pam_fscrypt module in fscrypt before 0.2.4 may incorrectly restore primary and supplementary group IDs to the values associated with the root user, which allows attackers to gain privileges via a successful login through certain applications that use Linux-PAM (aka pam).

CVE-2018-6558 has been assigned by security@ubuntu.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **The fscrypt Project** - **fscrypt** version **before 0.2.4**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Bug #1787548 “PAM fscrypt adds root(0) group to all users called...” : Bugs : fscrypt	Issue Tracking, Patch, Third Party Advisory	MISC launchpad.net/bugs/1787548

package : Ubuntu	launchpad.net text/html	
Ensure setting user privileges is reversible · google/fscrypt@3022c16 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/google/fscrypt/commit/3022c1603d968c22f147b4a2c49c4637dd1be91b
Ensure keyring privilege changes are reversible · google/fscrypt@315f9b0 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/google/fscrypt/commit/315f9b042237200174a1fb99427f74027e191d66
pam_fscrypt messes up user groups during login · Issue #77 · google/fscrypt · GitHub	Issue Tracking Third Party Advisory github.com text/html	MISC github.com/google/fscrypt/issues/77

Related QID Numbers

982075 Go (go) Security Update for github.com/google/fscrypt/security (GHSA-qj26-7grj-whg3)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Fscrypt	All	All	All	All
Application	Google	Fscrypt	All	All	All	All

cpe:2.3:a:google:fscrypt:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:fscrypt:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→