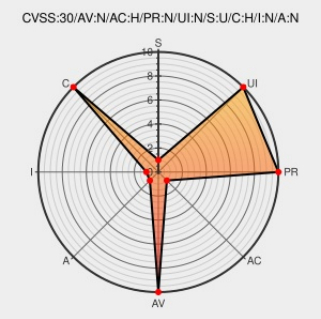
CVE-2019-7628

Published on: 02/07/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:51 PM UTC

CVE-2019-7628

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



Certain versions of Pagure from Redhat contain the following vulnerability:

Pagure 5.2 leaks API keys by e-mailing them to users. Few e-mail servers validate TLS certificates, so it is easy for man-in-the-middle attackers to read these e-mails and gain access to Pagure on behalf of other users. This issue is found in the API token expiration reminder cron job in files/api_key_expire_mail.py; disabling that job is also a viable solution. (E-mailing a substring of the API key was an attempted, but rejected, solution.)

CVE-2019-7628 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.9 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
Page not found :'(· Pagure.io	Broken link	MISC pagure.io/pagure/issue/4252

Page not found :(- Pagure.io	Broken Link pagure.io text/html Inactive Link Not Archived	MISC pagure.io/pagure/issue/4253
Issue #4230: API Key reminder sends the key in the clear via email - pagure - Pagure.io	Issue Tracking Patch Vendor Advisory pagure.io text/html	MISC pagure.io/pagure/issue/4230
PR#4254: CVE-2019-7628: Do not leak partial API keys. - pagure - Pagure.io	Issue Tracking Patch Vendor Advisory pagure.io text/html	MISC pagure.io/pagure/pull-request/4254
Commit - pagure - 9905fb1e64341822366b6ab1d414d2baa230af0a - Pagure.io	Issue Tracking Patch Vendor Advisory pagure.io text/html	MISC pagure.io/pagure/c/9905fb1e64341822366b6ab1d414d2baa2
Issue #4252: CVE-2019-7628: Pagure 5.2 leaks full API keys. - pagure - Pagure.io	Broken Link pagure.io text/html	MISC pagure.io/pagure/issue/4252

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Pagure	5.2	All	All	All
Application	Redhat	Pagure	5.2	All	All	All

cpe:2.3:a:redhat:pagure:5.2:*:*:*:*:*:*:*

cpe:2.3:a:redhat:pagure:5.2:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report