



CVE-2012-6140

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

Summary

CVE	CVE-2012-6140
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-04-24 10:28:00 UTC
Updated	2013-05-07 04:00:00 UTC
Description	pam_google_authenticator.c in the PAM module in Google Authenticator before 1.0 requires user-readable permissions for

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Authenticator	0.86	All	All	All
Application	Google	Authenticator	0.87	All	All	All
Application	Google	Authenticator	All	All	All	All
Application	Google	Authenticator	0.86	All	All	All
Application	Google	Authenticator	0.87	All	All	All

References

Reference	Source
oss-security - Re: CVE-2012-XXYY Request -- google-authenticator: Information disclosure due insecure requirement on the secrets file	ML
#666129 - new upstream version fixes security problem with the secret file (CVE-2012-6140) - Debian Bug report logs	CC
c3414e9857ad - google-authenticator - Two-step verification - Google Project Hosting	CC
953505 - (CVE-2012-6140) CVE-2012-6140 google-authenticator: Information disclosure due insecure requirement on the secrets file	CC
CVE Program record	CV
NVD vulnerability detail	NV

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](#)