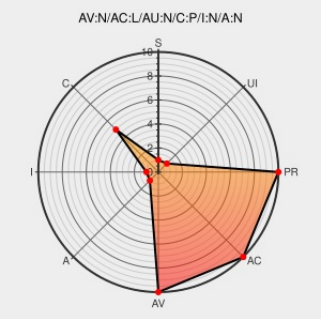
CVE-2012-2387

Published on: 08/20/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:26 PM UTC

CVE-2012-2387

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



Certain versions of Devotee from Debian contain the following vulnerability:

devotee 0.1 patch 2 uses a 32-bit seed for generating 48-bit random numbers, which makes it easier for remote attackers to obtain the secret monikers via a brute force attack.

CVE-2012-2387 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
oss-security - Re: CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions	www.openwall.com text/html	MLIST [oss-security] 20120521 Re: CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions
oss-security - CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions	www.openwall.com text/html	MLIST [oss-security] 20120518 CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions
oss-security - Re: CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions	www.openwall.com text/html	MLIST [oss-security] 20120522 CVE id request: devotee (debian vote engine) cryptographically weak random numbers permit discovery of secret ballot submissions

would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Debian	Devotee	0.1	All	All	All
Application	Debian	Devotee	0.1	All	All	All

cpe:2.3:a:debian:devotee:0.1:*:*:*:*:*:*:*:

cpe:2.3:a:debian:devotee:0.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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