

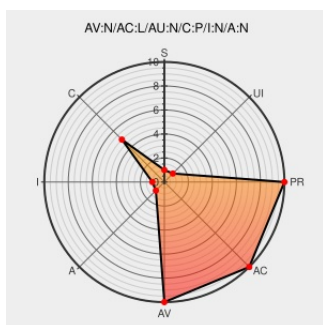


CVE-2012-3287

Published on: 06/13/2012 12:00:00 AM UTC

Last Modified on: 02/14/2023 07:15:00 AM UTC

CVE-2012-3287

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Md5crypt](#) from [Poul-henning Kamp](#) contain the following vulnerability:

Poul-Henning Kamp md5crypt has insufficient algorithmic complexity and a consequently short runtime, which makes it easier for context-dependent attackers to discover cleartext passwords via a brute-force attack, as demonstrated by an attack using GPU hardware.

CVE-2012-3287 has been assigned by [M](#) cve@mitre.org 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

Md5crypt Password scrambler is no longer considered safe by author — PHKs Bikeshed

[phk.freebsd.dk](#)
[text/html](#)

MISC
phk.freebsd.dk/sagas/md5crypt_eol/

Md5crypt Password scrambler is no longer considered safe by author — PHKs Bikeshed

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

CONFIRM
phk.freebsd.dk/sagas/md5crypt_eol.html

Inactive Link **Not Archived**

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that 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	Poul-henning Kamp	Md5crypt	-	All	All	All
Application	Poul-henning Kamp	Md5crypt	-	All	All	All
cpe:2.3:a:poul-henning_kamp:md5crypt:-:*:*:*:*:*:						
cpe:2.3:a:poul-henning_kamp:md5crypt:-:*:*:*:*:*:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		