

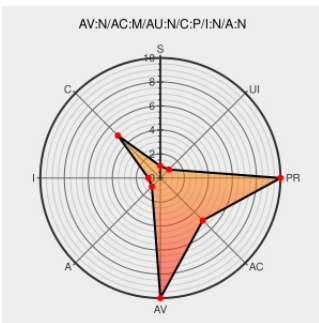


CVE-2011-3189

Published on: 08/25/2011 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:19 AM UTC

CVE-2011-3189

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

Certain versions of [Php](#) from [Php](#) contain the following vulnerability:

The crypt function in PHP 5.3.7, when the MD5 hash type is used, returns the value of the salt argument instead of the hashed string, which might allow remote attackers to bypass authentication via an arbitrary password, a different vulnerability than CVE-2011-2483.

CVE-2011-3189 has been assigned by  secalert@redhat.com to track the vulnerability

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

APPLE-SA-2012-02-01-1 OS X Lion v10.7.3 and Security Update 2012-001

[lists.apple.com](#)
[text/html](#)

 [APPLE APPLE-SA-2012-02-01-1](#)

380261 – (CVE-2011-3189) =dev-lang/php-5.3.7: crypt() returns only the salt for MD5 (CVE-2011-3189)

[bugs.gentoo.org](#)
[text/html](#)

 [CONFIRM bugs.gentoo.org/show_bug.cgi?id=380261](#)

oss-security - CVE assignment - PHP salt flaw CVE-2011-3189

[www.openwall.com](#)
[text/html](#)

 [MLIST \[oss-security\] 20110823 CVE assignment - PHP salt flaw CVE-2011-3189](#)

No Description Provided

[osvdb.org](#)

 [OSVDB 74726](#)

Inactive Link **Not Archived**

PHP :: Bug #55439 :: crypt() returns only the salt for MD5

[Exploit bugs.php.net](#)

 [CONFIRM bugs.php.net/bug.php?id=55439](#)

	text/xml	
PHP: News Archive - 2011	www.php.net text/html	 CONFIRM www.php.net/archive/2011.php?id2011-08-23-1
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF php-crypt-security-bypass(69429)
PHP: PHP 5 ChangeLog	www.php.net text/html	 CONFIRM www.php.net/ChangeLog-5.php#5.3.8
About the security content of OS X Lion v10.7.3 and Security Update 2012-001	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT5130
PHP "crypt()" MD5 Salt Security Issue - Secunia.com	Vendor Advisory web.archive.org text/html	 SECUNIA 45678

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	Php	Php	5.3.7	All	All	All
Application	Php	Php	5.3.7	All	All	All
cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:						
cpe:2.3:a:php:php:5.3.7:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)