

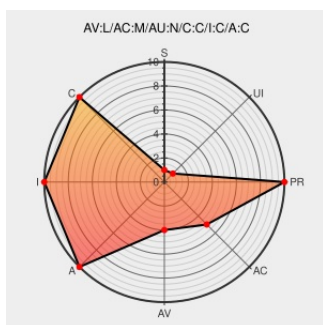


CVE-2007-1401

Published on: 03/10/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:36 PM UTC

CVE-2007-1401

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

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

Buffer overflow in the crack extension (CrackLib), as bundled with PHP 4.4.6 and other versions before 5.0.0, might allow local users to gain privileges via a long argument to the crack_opendict function.

CVE-2007-1401 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **6.9 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

PHP 4.4.6 - 'crack_opendict()' Local Buffer Overflow - Windows local Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 3431](#)

Error 404 :(

[Exploit](#)
[retrogod.altervista.org](#)
[text/plain](#)
[Inactive Link](#) [Not Archived](#)

MISC
[retrogod.altervista.org/php_446_crack_opendict_local_bof.html](#)

CXSecurity - IDS

[securityreason.com](#)
[text/html](#)

[SREASON 2405](#)

SecurityFocus

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

[BUGTRAQ 20070308 PHP 4.4.6 crack_opendict\(\) local buffer overflow poc exploit](#)

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	4.4.6	All	All	All
Application	Php	Php	4.4.6	All	All	All
cpe:2.3:a:php:php:4.4.6:*****:						
cpe:2.3:a:php:php:4.4.6:*****:						

← Previous ID

Next ID→