



CVE-2007-4528

Published on: 08/24/2007 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:31 PM UTC

CVE-2007-4528

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

The Foreign Function Interface (ffi) extension in PHP 5.0.5 does not follow `safe_mode` restrictions, which allows context-dependent attackers to execute arbitrary code by loading an arbitrary DLL and calling a function, as demonstrated by `kernel32.dll` and the `WinExec` function. NOTE: this issue does not cross privilege boundaries in most contexts, so perhaps it should not be included in CVE.

CVE-2007-4528 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
PHP FFI Extension 5.0.5 Local Safe_mode Bypass Exploit	www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 4311

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	5.0.5	All	All	All
Application	Php	Php	5.0.5	All	All	All
cpe:2.3:a:php:php:5.0.5:*****:						
cpe:2.3:a:php:php:5.0.5:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID				Next ID→		