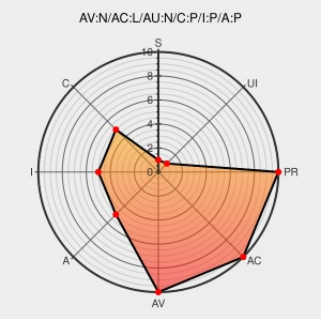
CVE-2005-2314

Published on: 07/19/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2314

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



Certain versions of Phpsftpd from Phpsftpd contain the following vulnerability:

inc.login.php in PHPsFTPd 0.2 through 0.4 allows remote attackers to obtain the administrator's username and password by setting the do_login parameter and performing an edit action using user.php, which causes the login check to be bypassed and leaks the password in the response.

CVE-2005-2314 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
PHPsFTPd Inc.Login.PHP Privilege Escalation Vulnerability	Exploit, Patch, cve.report (archive), text/html	BID 14222
	Exploit, Vendor Advisory, packetstorm.linuxsecurity.com, text/x-c, Inactive Link, Not Archived	MISC packetstorm.linuxsecurity.com/0507-exploits/phpsftpd.txt
RUS-CERT - Requested Page not found	cert.uni-stuttgart.de, text/html, Inactive Link, Not Archived	BUGTRAQ 20050713 PHPsFTPd - Admin password leak

Secunia - Advisories - PHPsFTPd "do_login" Authentication Bypass Vulnerability	Vendor Advisory web.archive.org text/html	SECUNIA 15879
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2005-1101
PHPsFTPd Grants Administrative Access to Remote Users - SecurityTracker	securitytracker.com text/html	SECTRACK 1014481

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	Phpsftpd	Phpsftpd	0.2	All	All	All
Application	Phpsftpd	Phpsftpd	0.4	All	All	All
Application	Phpsftpd	Phpsftpd	0.2	All	All	All
Application	Phpsftpd	Phpsftpd	0.4	All	All	All

cpe:2.3:a:phpsftpd:phpsftpd:0.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpsftpd:phpsftpd:0.4:*:*:*:*:*:*:*:

cpe:2.3:a:phpsftpd:phpsftpd:0.2:*:*:*:*:*:*:*:

cpe:2.3:a:phpsftpd:phpsftpd:0.4:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→