

Re: Hacked by aLpTurkTegin, help patching this hole

Re: Hacked by aLpTurkTegin, help patching this hole

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2008-05/msg00119.html>

- *From:* "Utmost Bastard" <utmostbastard@xxxxxxxx>
 - *Date:* Wed, 21 May 2008 14:26:16 -0400
-

Could be any of the following...

- 1) If co-hosted any of the other sites could have been compromised.
- 2) Writeable dir anywhere
- 3) SQL injected shell
- 4) Exploitable script/program
- 5) Missing patches
- 6) Easily cracked user/pass/service account
- 7) Misconfiguration in just about anything
- 8) About 100000 other things.

You must be more specific. Provide logs, patch level, version levels, scripts used, check dir permissions, state type of hosting etc.....

----- Original Message ----- From: "Mifa" <mifa@xxxxxxxxxxxxxxxxxxxx>
To: <pen-test@xxxxxxxxxxxxxxxxxxxx>
Sent: Tuesday, May 20, 2008 8:46 AM
Subject: Hacked by aLpTurkTegin, help patching this hole

Our website was defaced by aLpTurkTegin. We are running apache, php ect. Does anyone know how this hacker is getting in and what I can do to prevent this?

Our main web directory had all but one file deleted and hackedIndex.php, a.asp(a 0 byte file) and trustscn_put_test2 were placed into the main directory. The fact that the webserver served hackedindex.php makes me think its a apache web server flaw.

Any comments, suggestions?
Thanks, -D

This list is sponsored by: Cenxic

Top 5 Common Mistakes

Re: Hacked by aLpTurkTegin, help patching this hole

Re: Hacked by aLpTurkTegin, help patching this hole

in Securing Web Applications
Find out now! Get Webinar Recording and PPT Slides

www.cenzic.com/landing/securityfocus/hackinar

This list is sponsored by: Cenzic

Top 5 Common Mistakes in Securing Web Applications Find out now! Get Webinar Recording and PPT Slides

www.cenzic.com/landing/securityfocus/hackinar
