

[UNIX] Password Disclosure Vulnerability Found in ChitChat

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-03/0064.html>

From: support@securiteam.com

Date: 03/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Mar 2003 11:40:41 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

In the US?

Contact Beyond Security at our new California office housewarming rates on automated network vulnerability scanning. We also welcome ISPs and other resellers!

Please contact us at: 323-882-8286 or ussales@beyondsecurity.com

Password Disclosure Vulnerability Found in ChitChat

SUMMARY

<<http://www.cyber-cats.com/php/>> The PHP ChitChat Message Board (GuestBook) script allows a number of options.

Admin functions include the ability to easily remove posts, delete entire archives, change password, block IP addresses, and administer "bad language" filtering.

The script is mis-configured to allow remote users to access sensitive files including administrator's login and password information.

DETAILS

Vulnerable versions:

* ChitChat Version 3.00 and prior.

The vulnerability allows any user to access the passwd.txt file where the login name and password are kept. The passwords are DES encrypted, but that can be decrypted using various hacking tools.

Securiteam: [UNIX] Password Disclosure Vulnerability Found in ChitChat

Exploit Method:

Simply go to:

http://[vulnerable.site.address]/[public | cgi-bin dir]/files/passwd.txt

ADDITIONAL INFORMATION

Information was provided by <mailto:r2subj3ct@dwclan.org> subj

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.