

[UNIX] Poster Version.two Privilege Escalation

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-05/0044.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 05/21/03

To: list@securiteam.com

Date: 21 May 2003 17:49:32 +0200

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

Poster Version.two Privilege Escalation

SUMMARY

<<http://x.faction.nu/>> Poster is a "News Management Script. Uses flat text files, very easy to install, add/edit/remove users, add/edit/remove entries". A vulnerability in the product allows under privileged users to gain elevated privileges.

DETAILS

If a user has their account type set to 'normal' by the administrator, then they cannot edit other people's accounts, nor can they edit other people's posts, they are harmless to the site.

Sadly, there is a dangerous vulnerability within the 'index.php' file in the 'edit account' section of the code, which places data from the username, password, and email address fields straight into the 'mem.php' (user password and privileges) file.

A normal 'mem.php' file looks like this:

<?

Securiteam: [UNIX] Poster Version.two Privilege Escalation

```
James|password|email@address.com|admin|  
Jack|password|email@address.com|normal|  
?>
```

Where James has an administrator account and Jack does not.

The normal user, Jack, could decide to change his account details to:

```
Username: Jack  
Password: password  
Email: email@address.com|admin|
```

Notice the '|admin|' appended to the end of the address. When Jack saved his details, his account would appear as:

```
Jack|password|email@address.com|admin||normal|
```

The 'index.php' file would take the first four parameters as the account details and type, then seeing that parameter four was '|admin|', it would assign Jack administrator privileges.

Jack could then delete all the posts and accounts on the site when he next logged in.

ADDITIONAL INFORMATION

The information has been provided by <mailto:peter4020@hotmail.com> Peter Winter-Smith.

=====

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.