

[UNIX] JSBoard Arbitrary File Reading

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-01/0096.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/23/05

To: list@securiteam.com

Date: 23 Jan 2005 16:07:40 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

JSBoard Arbitrary File Reading

SUMMARY

<<http://kldp.net/projects/jsboard/>> JSBoard is "one of most widely used web BBS applications in Korea".

Due to improper input filtering by JSBoard a remote attacker can include arbitrary local files in the response the server returns, thus disclosing them.

DETAILS

Vulnerable Systems:

- * JSBoard version 2.0.9 and prior

Immune Systems:

- * JSBoard version 2.0.10 or newer

PHP has a feature that will discard any input values containing NULL characters whenever the item `magic_quotes_gpc` has been set to off. Because JSBoard `session.php` doesn't sanitize the `$table` variable, a malicious attacker can use it read arbitrary files.

Vulnerable code:

Securiteam: [UNIX] JSBoard Arbitrary File Reading

```
include_once "include/print.php";  
parse_query_str();  
$opt = $table ? "&table=$table" : "";  
$opts = $table ? "?table=$table" : "";  
..snip...
```

Proof of Concept:

[http://\[victim\]/session.php?logins=true&m=logout&table=../../../../../../../../etc/passwd%00](http://[victim]/session.php?logins=true&m=logout&table=../../../../../../../../etc/passwd%00)

Solution:

Upgrade to JSBoard version 2.0.10 or newer, available from:

<<http://kldp.net/frs/download.php/1729/jsboard-2.0.10.tar.gz>>

<http://kldp.net/frs/download.php/1729/jsboard-2.0.10.tar.gz>

Disclosure Timeline:

2004-12-31 Vulnerability found.
2004-12-31 JSBoard developer notified.
2005-01-02 Developer confirmed.
2005-01-02 Update version released.
2005-01-20 Official release.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:advisory@stgsecurity.com>>
SSR Team.

=====

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.