

[UNIX] Blog Torrent Arbitrary File Downloading

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0047.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 12/16/04

To: list@securiteam.com

Date: 16 Dec 2004 15:01:36 +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>

Blog Torrent Arbitrary File Downloading

SUMMARY

Blogtorrent is "a collection of PHP scripts that are designed to make it simple to host files for transfer via bittorrent". One of the scripts in the Blogtorrent doesn't correctly sanitize it's inputs, before using one of them to read and serve a file from the local system.

DETAILS

Vulnerable Systems:

- * Blog Torrent preview version 0.8

The above mentioned vulnerability can be exploited to remotely download any file upon the web server that is readable by the UID that the web server is running as.

The code in question is contained in btdownload.php and looks like this:

```
echo file_get_contents('torrents/'.$_GET['file']);
```

Exploit:

The following URL can be used to download a file:

<http://example/battletorrent/btdownload.php?type=torrent&file=../../etc/passwd> (Adjust the ".."s and the filename to suit your taste).

Securiteam: [UNIX] Blog Torrent Arbitrary File Downloading

Fix:

While no new release is planned to address this hole the authors did commit a simple fix to their CVS repository.

This can be obtained from here:

http://cvs.sourceforge.net/viewcvs.py/battletorrent/btorrent_server/btdownload.php?r1=1.6&r2=1.7
http://cvs.sourceforge.net/viewcvs.py/battletorrent/btorrent_server/btdownload.php?r1=1.6&r2=1.7

(The patch was committed less than a day after the hole was privately reported to them, making them a responsive bunch).

ADDITIONAL INFORMATION

The information has been provided by <mailto:steve@steve.org.uk> Steve Kemp.

=====

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.