

[NT] Technical Details of BadBlue EXT.DLL Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0025.html>

From: support@securiteam.com

Date: 07/09/02

From: support@securiteam.com

To: list@securiteam.com

Date: Tue, 9 Jul 2002 08:08:05 +0200 (CEST)

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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

Technical Details of BadBlue EXT.DLL Vulnerability

SUMMARY

<<http://www.badblue.com/>> BadBlue is a file sharing web server. A vulnerability exists in how EXT.DLL sanitizes input for HTX/HTS pages. Any user input is inserted un-sanitized, making any HTX or HTS pages that display output vulnerable to attack.

DETAILS

Vulnerable systems:

- * BadBlue version 1.7.2 and prior

Immune systems:

- * BadBlue version 1.7.3

Example:

Webmasters can test for the vulnerability by running a search query containing HTML/script (e.g. "alert('vulnerable!');" would do, note that we replaced the 'i' with '!').

If the search results page displays a JavaScript Alert, your server could be used in attacks against visiting browsers.

Securiteam: [NT] Technical Details of BadBlue EXT.DLL Vulnerability

ADDITIONAL INFORMATION

The information has been provided by <mailto:mattmurphy@kc.rr.com>
Matthew Murphy.

=====

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.

-
- **Previous message:** support@securiteam.com: "[NT] Buffer Overflow in MyWebServer"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)