

[NT] BadBlue 302 Status Message XSS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0095.html>

From: support@securiteam.com

Date: 07/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 22 Jul 2002 22:06:59 +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.

BadBlue 302 Status Message XSS

SUMMARY

BadBlue is susceptible to a cross-site scripting attack in its HTTP Redirection response. The attack would allow attackers to present data as if it was sent from the server (HTML and JavaScript content).

DETAILS

Vulnerable systems:

- * BadBlue version 1.74

When BadBlue is passed a name of a non-existent file path (or an existent folder) that does not end in a 0x2F, character ("/") it returns a 302-status code containing some text:

HTTP/1.0 302 found

Location: /<SCRIPT>/

```
<html><body><pre>GET /<SCRIPT> HTTP/1.0
```

Obviously, if you pass in HTML markup, it continues into the reply un-filtered, resulting in a cross-site scripting attack.

Securiteam: [NT] BadBlue 302 Status Message XSS

This vulnerability cannot be exploited on Internet Explorer, or any browser that ignores entities in HTTP redirect messages.

Successful exploitation may require a significant amount of "garbage" HTML, as the entity is downloaded, displayed, and then the redirect executed. This vulnerability poses minimal risk, but should be taken very seriously.

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: "[UNIX] IBM Tivoli Management Framework Buffer Overflow (ManagedNode)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)