

# [NT] BadBlue File Viewing Vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0089.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/23/01

From: [support@securiteam.com](mailto:support@securiteam.com)

To: [list@securiteam.com](mailto:list@securiteam.com)

Subject: [NT] BadBlue File Viewing Vulnerability

Message-Id: <20010823142330.335C2138BF@mail.der-keiler.de>

Date: Thu, 23 Aug 2001 16:23:30 +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 File Viewing Vulnerability

---

## SUMMARY

<<http://www.badblue.com/prodpe.htm>> BadBlue PE provides searching, sharing, peer-to-peer (P2P) and customizability in a tiny footprint. A security vulnerability in the product allows attackers to view the source code of PHP files (and download DLLs) by issuing a special HTTP request.

## DETAILS

Vulnerable systems:

BadBlue version 1.02 and prior

Immune systems:

BadBlue version 1.5

BadBlue contains an input validation vulnerability that may lead to download the full source code of .PHP pages. This is due to a lack of checks for NULL bytes.

Example:

<http://example.com/test.php%00>

Securiteam: [NT] BadBlue File Viewing Vulnerability

Note: It is possible to download .DLL file.

Example:

<http://example.com/ext.dll%00>

ADDITIONAL INFORMATION

The information has been provided by

<<mailto:aurelien.cabazon@iSecureLabs.com>> acz [iSecureLabs].

=====

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](mailto:list-unsubscribe@securiteam.com)

In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NEWS] The Perfect Read Receipt – Using HTML Tagging to Verify E-mail Reading ("Web Bugs")"
  - **Messages sorted by:** [\[ date \] \[ thread \] \[ subject \] \[ author \] \[ attachment \]](#)