

# [NT] Unchecked Buffer in Jana Web Server (Method)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0043.html>

---

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

*Date:* 08/13/02

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

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

Date: Tue, 13 Aug 2002 15:45:25 +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.

-----

Unchecked Buffer in Jana Web Server (Method)

---

## SUMMARY

<<http://www.janaserver.de/en/>> Jana Web Server has been the focus of several recent discoveries, including several buffer overrun vulnerabilities. Yet another exploitable overflow exists in the Jana Web Server. Jana Web Server does not properly check the size of the HTTP request method input by the user before storing it, resulting in a stack overflow.

If the method sufficiently exceeds the allocated storage, EIP will be overwritten.

## DETAILS

Vulnerable systems:

\* Jana Server version 2.2.1

Example:

The overflow occurs whenever the following

[buffer] / HTTP/1.0

Securiteam: [NT] Unchecked Buffer in Jana Web Server (Method)

Is sent to the server, note that the buffer cannot contain any of the following chars: 0x00, 0x0D, 0x0A, and 0x20.

ADDITIONAL INFORMATION

The information has been provided by <mailto:[mattmurphy@kc.rr.com](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](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] SNMP Vulnerability in Avaya Cajun"
  - *Messages sorted by:* [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)