

# [NT] IBM WebSphere Large Header DoS

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0075.html>

---

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

*Date:* 09/22/02

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

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

Date: Sun, 22 Sep 2002 13:10:04 +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.

-----

IBM WebSphere Large Header DoS

---

## SUMMARY

A malicious user can issue a malformed HTTP request and cause the web server to crash.

## DETAILS

Vulnerable systems:

- IBM WebSphere 4.0.3 on Windows 2000 Server

The application does not perform proper bounds check on large HTTP headers, and as a result, the application can be crashed by a remote user. It could not be established if this could lead to code execution.

If a request is made for a .JSP resource (the .JSP file does not need to exist), and the HTTP field "Host" contains 796 characters or more, the web service will crash. Other HTTP fields are also vulnerable if the size is increased to 4K.

The web service sometimes recovers on its own.

Vendor URL:

You can visit the vendor webpage here: [<http://www.ibm.com>](http://www.ibm.com)

<http://www.ibm.com>

Securiteam: [NT] IBM WebSphere Large Header DoS

Vendor response:

The vendor was notified on 4 June 2002. On 12 July, the vendor sent us a patch for the problem. On 19 September, we confirmed that the patch was officially released.

Corrective action:

Install PQ62144 (supercedes PQ62249). The URL is wrapped:

<<http://www-1.ibm.com/support/docview.wss?rs=180=PQ62144/a>>>  
<http://www-1.ibm.com/support/docview.wss?rs=180=PQ62144/a>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pgrundl@kpmg.dk>> Peter Gründl.

=====

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] Firewall-1 HTTP Security Server – Proxy Vulnerability"
  - **Messages sorted by:** [ date ] [ thread ] [ subject ] [ author ] [ attachment ]