

[VulnWatch] KPMG-2002031: Jigsaw Webserver Path Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-07/0032.html>

From: Peter Gründl (pgrundl@kpmg.dk)
Date: 07/17/02

From: Peter Gründl <pgrundl@kpmg.dk>
To: "vulnwatch" <vulnwatch@vulnwatch.org>
Date: Wed, 17 Jul 2002 11:27:11 +0200

Title: Jigsaw Webserver Path Disclosure

BUG-ID: 2002031
Released: 17th Jul 2002

Problem:

=====

It is possible to disclose the physical path to the webroot. This information could be useful to a malicious user wishing to gain illegal access to resources on the server.

Vulnerable:

=====

- Jigsaw V2.2.1 Distribution on Windows 2000 Server

Not Vulnerable:

=====

- Jigsaw V2.2.1 Dev/2.2/20020711 on Windows 2000 Server

Product Description:

=====

Quoted from the vendor webpage:

"Jigsaw is W3C's leading-edge Web server platform, providing a sample HTTP 1.1 implementation and a variety of other features on top of an advanced architecture implemented in Java. The W3C Jigsaw Activity statement explains the motivation and future plans in more detail. Jigsaw is an W3C Open Source Project, started May 1996."

Details:

=====

VulnWatch: [VulnWatch] KPMG-2002031: Jigsaw Webserver Path Disclosure

Requesting /aux two times, results in an error message, after second request, containing the physical path to the web root.

Vendor URL:

=====

You can visit the vendor webpage here: <http://www.w3.org>

Vendor response:

=====

The vendor was notified on the 27th of May, 2002. On the 11th of July, 2002 we verified that the issue was corrected in the latest build (20020708).

Corrective action:

=====

Upgrade your Jigsaw.jar to the latest build, available from:
<http://jigsaw.w3.org/Devel/classes-2.2/20020711/>

Author: Peter Gründl (pgrundl@kpmg.dk)

KPMG is not responsible for the misuse of the information we provide through our security advisories. These advisories are a service to the professional security community. In no event shall KPMG be liable for any consequences whatsoever arising out of or in connection with the use or spread of this information.

-
- **Previous message:** [Sym Security: "Re: \[VulnWatch\] Advisory Name: Norton Personal Internet Firewall HTTP Proxy Vulnerability"](#)
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)