

[NT] Resin Large Parameter Denial of Service

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0061.html>

From: support@securiteam.com

Date: 06/17/02

From: support@securiteam.com

To: list@securiteam.com

Date: Mon, 17 Jun 2002 20:36:01 +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.

Resin Large Parameter Denial of Service

SUMMARY

It is possible for a malicious user to cause a Denial of Service by requesting certain malformed URLs from the <http://www.caucho.com> Resin web server.

DETAILS

Vulnerable systems:

- * Resin 2.1.1 standalone on Windows 2000 Server

Immune systems:

- * Resin 2.1.2 standalone on Windows 2000 Server

By defining large variables when accessing non-existent resources, it is possible to consume the entire workspace on the server. This will result in hanging parts of or the entire web server.

Vendor Response:

This was reported to the vendor on the 22nd of May, 2002. On the 11th of June, 2002 the vendor released a new version that corrects the issue.

Corrective action:

Upgrade to version 2.1.2 available from:

Securiteam: [NT] Resin Large Parameter Denial of Service

<<http://www.caucho.com/download/>> <http://www.caucho.com/download/>

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

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: "[\[NT\] Heap Overrun in HTR Chunked Encoding Could Enable Web Server Compromise](#)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)