

[NT] Multiple vulnerabilities in New Atlanta ServletExec ISAPI

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-05/0093.html>

From: support@securiteam.com

Date: 05/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 22 May 2002 22:12:17 +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.

Multiple vulnerabilities in New Atlanta ServletExec ISAPI

SUMMARY

<<http://www.newatlanta.com/products/servletexec/index.jsp>> ServletExec 4.1 ISAPI is a Java Servlet/JSP Engine for Internet Information Server and is implemented as an ISAPI filter. The JSP functionality is provided by a servlet which is enabled by default and contains three security flaws.

DETAILS

Vulnerable systems:

* New Atlanta ServletExec ISAPI version 4.1

1. ServletExec discloses physical path of web root

It is possible to invoke the class

'com.newatlanta.servletexec.JSP10Servlet' directly by requesting a URL

such as:

/servlet/com.newatlanta.servletexec.JSP10Servlet/

If no filename is supplied to it, then it returns an error message:

Error. The file was not found. (filename =

f:\inetpub\wwwroot\servlet\com.newatlanta.servletexec.JSP10Servlet)

Securiteam: [NT] Multiple vulnerabilities in New Atlanta ServletExec ISAPI

Disclosing the physical path of the web root.

2. JSP10Servlet allows files to be read from within IIS web root
By invoking the JSP10Servlet (or simply JSPServlet) using the URL described above, it is possible to read files from within the web root. It did not appear to be possible to 'break out' of the web root and read files from other parts of the file system. The path must be URL encoded for this to work. For instance, a request such as:
/servlet/com.newatlanta.servletexec.JSP10Servlet/..%5c..%5c\global.asa

Will retrieve the global.asa file, which is normally not served.

3. DoS via overly long request for .JSP file
By making a request for an overly long named .jsp file, Internet Information Server can be crashed.

The denial of service condition can be triggered by either requesting an overly long named .jsp file:
/servlet/AAAAAAAAAAAAAAAAAAAA....AAAAAAAAAAAAAAAAAAAA.jsp

Or by invoking the JSPServlet or JSP10Servlet directly:
/servlet/com.newatlanta.servletexec.JSPServlet/AAAAAAAAAAAA....AAAA

Patch Information:

There is a workaround for the physical path disclosure bug, which should be in the FAQ's at

<http://www.newatlanta.com/products/servletexec/self_help/faq_list.jsp>
http://www.newatlanta.com/products/servletexec/self_help/faq_list.jsp

The other issues are fixed in Patch #9 from
<ftp://ftp.newatlanta.com/public/4_1/patches/>
ftp://ftp.newatlanta.com/public/4_1/patches/

ADDITIONAL INFORMATION

The information has been provided by <mailto:matt@westpoint.ltd.uk> Matt Moore.

=====

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,

Securiteam: [NT] Multiple vulnerabilities in New Atlanta ServletExec ISAPI

loss of business profits or special damages.

- **Previous message:** support@securiteam.com: "[NEWS] Multiple Vulnerabilities in Cisco IP Telephones"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)