

[NEWS] Apache Cocoon Directory Traversal Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0101.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/23/03

To: list@securiteam.com

Date: 23 Oct 2003 14:05:45 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Apache Cocoon Directory Traversal Vulnerability

SUMMARY

<<http://cocoon.apache.org>> Apache Cocoon is "an Open Source web development framework built around the concepts of separation of concerns and component-based web development.

Cocoon implements these concepts around the notion of 'component pipelines', each component on the pipeline specializing on a particular operation. This makes it possible to use a Lego-like approach in building web solutions, hooking together components into pipelines without any required programming.

Cocoon is "web glue for your web application development needs". It is a glue that keeps concerns separate and allows parallel evolution of all aspects of a web application, improving development pace and reducing the chance of conflicts".

Apache Cocoon's sample files have been found to be vulnerable to a directory traversal (in the "view source" functionality).

DETAILS

Securiteam: [NEWS] Apache Cocoon Directory Traversal Vulnerability

Vulnerable systems:

- * Apache Cocoon version 2.1.2 (Release)
- * Apache Cocoon version 2.1 before 22 Oct 2003 12:00
- * Apache Cocoon version 2.2 (Development) before 22 Oct 2003 12:00

Immune systems:

- * Apache Cocoon version 2.1 after 22 Oct 2003 12:00
- * Apache Cocoon version 2.2 (Development) after 22 Oct 2003 12:00

Mitigating factors:

- * On a production system samples should NEVER be installed
- * Setting correct files permission should reduce the risk of this thread

Exploit:

On a Windows host, where Cocoon is installed on the C:\cocoon\, accessing <http://a.Host.com:8888/samples/view-source?filename=../../boot.ini> will initiate the download of the c:\boot.ini file.

Disclosure timeline:

20 Oct 2003 17:45 Bug reported on
<http://nagoya.apache.org/bugzilla/show_bug.cgi?id=23949>
http://nagoya.apache.org/bugzilla/show_bug.cgi?id=23949
20 Oct 2003 22:38 Problem acknowledged by Jörg Heinicke.
22 Oct 2003 11:59 Problem fixed in CVS by Jörg Heinicke.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:thierry.deleeuw@advalvas.be>>
Thierry De Leeuw.

=====

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.