

[NEWS] Cross-Site Scripting in Aestiva's HTML/OS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-09/0016.html>

From: support@securiteam.com

Date: 09/05/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 5 Sep 2002 15:27:46 +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.

Cross-Site Scripting in Aestiva's HTML/OS

SUMMARY

<<http://www.aestiva.com/pages/html/02943.1.1019246789336614088>> Aestiva HTML/OS is a high-performance database engine and development suite for building advanced web sites and web-based software products. The product has been found to contain a security vulnerability that allows remote attackers to cause it to display third party data as if it were its own.

DETAILS

The Aestiva HTML/OS CGIs has been found to be vulnerable to XSS due to poor error reporting (no meta-character filtering).

Anything you want can be appended to any URL ending in '/' in an area of the website where HTML/OS is handling the request. The resulting error message will echo back the unfiltered request.

Examples:

EAX will refrain from listing real-world examples

(s/www.example.com/<target>):

Securiteam: [NEWS] Cross-Site Scripting in Aestiva's HTML/OS

[http://www.example.com/pages/htmllos/%3Cscript%3Ealert\(document.domain\);%3C/script%3E](http://www.example.com/pages/htmllos/%3Cscript%3Ealert(document.domain);%3C/script%3E)
[http://www.example.com/cgi-bin/erba/start/%3Cscript%3Ealert\(document.domain\);%3C/script%3E](http://www.example.com/cgi-bin/erba/start/%3Cscript%3Ealert(document.domain);%3C/script%3E)
[http://www.exmaple.com/cgi-bin/start.cgi/%3Cscript%3Ealert\(document.domain\);%3C/script%3E](http://www.exmaple.com/cgi-bin/start.cgi/%3Cscript%3Ealert(document.domain);%3C/script%3E)

Thousands of websites are currently vulnerable according to Google, including Aestiva.com.

Vendor status:
Has been notified but has not responded.

ADDITIONAL INFORMATION

The information has been provided by <mailto:eax@3xT.org> eax.

=====

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: "[UNIX] AFD Multiple Local Root Compromises"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)