

Securiteam: [UNIX] Xitami Errors.gsl Script Injection Vulnerabilities (GSL)

[UNIX] Xitami Errors.gsl Script Injection Vulnerabilities (GSL)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0109.html>

From: support@securiteam.com

Date: 06/23/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sun, 23 Jun 2002 21:02:45 +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.

Xitami Errors.gsl Script Injection Vulnerabilities (GSL)

SUMMARY

<<http://www.imatix.com/>> Xitami is a multithreaded Web server. Though small and simple, Xitami is robust enough to handle high-volume intranets. Built from the ground up as a high-performance Web server engine, it pumps data onto the network at top speed. This means that it can serve large files quickly while handling many simultaneous hits. A vulnerability in the product allows remote attackers to insert malicious HTML and JavaScript code into existing web pages.

DETAILS

Vulnerable systems:

- * Xitami 2.5 Beta

In Xitami, a GSL feature was implemented. GSL is an XML-type server-side language. Xitami demonstrates this with two sample scripts. Errors.gsl is used for error processing in servers where it has been enabled. (Disabled by default)

Errors.gsl poorly checks the hostname of the input request, only filtering SCRIPT (case insensitive filter) out of the host. Therefore, events can be

Securiteam: [UNIX] Xitami Errors.gsl Script Injection Vulnerabilities (GSL)

fired to run code:

[http://www.=""%20ONERROR=""alert\(document.cookie\)">.target.com/error404](http://www.=)

It also does not check the User-Agent field AT ALL:

```
[ telnet target.net 80 ]
GET / HTTP/1.0
User-Agent: <SCRIPT>alert(document.cookie);</SCRIPT>
[ End sent data ]
```

Xitami will return the script in the output. If an attacking page can control the User-Agent (or any part of it), it can run code on a visiting browser in the name of the site running the Beta.

Vendor status:

iMatix has forwarded my original post to the discussion forum, and will update the script in future beta releases.

ADDITIONAL INFORMATION

The information has been provided by <mailto:mattmurphy@kc.rr.com>
Matthew Murphy.

=====

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: "[TOOL] Blowchunks – Protecting Existing Apache Servers Until Upgrades Arrive"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)