

[NEWS] Xitami Malformed Header Request DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0102.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/26/03

To: list@securiteam.com

Date: 26 Nov 2003 19:03:53 +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>

Xitami Malformed Header Request DoS

SUMMARY

<<http://www.xitami.com/>> Xitami web server has been found to contain a vulnerability that allows remote attackers to cause a denial of service against the product by sending the server a malformed header.

DETAILS

Vulnerable systems:

- * Xitami version 2.5 and prior

Xitami has a logical error in the way it handles POST requests. A request like this will make the server not respond to any other requests although the server still listens to port 80:

POST /forum/index.php HTTP/1.1

Referer: Sentryunion

Accept-Encoding: None

User-Agent: Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)

Content-Length: 10

(Long string here)

0x0D 0x0A

(Another long string here)

Securiteam: [NEWS] Xitami Malformed Header Request DoS

Vulnerable code:

The code that handles parsing of the HTTP header doesn't have a good logic:

```
while(header && *header && *header != '\r')
{
  header_name = header
  if((header_value=strchr(header_name, ":")) != NULL)
  { ... header++;}
}
```

So if inside the HTTP request the header does not contain a ":" character, the while loop will run until the process is manually terminated.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:trihuynh@zeeup.com>> Tri Huynh.

=====

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.