

[NT] DeepMetrix LiveStats JavaScript Injection

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0085.html>

From: support@securiteam.com

Date: 06/19/02

From: support@securiteam.com

To: list@securiteam.com

Date: Wed, 19 Jun 2002 09:12:41 +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.

DeepMetrix LiveStats JavaScript Injection

SUMMARY

DeepMetrix (formerly MediaHouse) LiveStats is server software that provides an interactive web based summary of website traffic based on HTTP server logs. A security vulnerability in the product allows attackers to insert malicious JavaScript and HTML into existing web pages.

DETAILS

Vulnerable systems:

* LiveStats versions between 5.03 and 6.2.1

By crafting special user-agent or referer headers on HTTP requests to a web site that is monitored by LiveStats, arbitrary JavaScript can be executed in the browser of a person viewing the LiveStats HTML reports. LiveStats displays the browser-tag and referer strings in its reports verbatim, including any script tags. Script that discloses the URL of the LiveStats interface could allow access that is normally protected by a private ServerID.

Demonstration:

Browse <http://www.deepmetrix.com/> <http://www.deepmetrix.com/> with a user-agent of XXX<script>alert("foo");</script> Then browse the Demo of LiveStats available on the DeepMetrix web site at:

Securiteam: [NT] DeepMetrix LiveStats JavaScript Injection

<<http://lvestats.deepmetrix.com/stats?type=loginverid=deepmetrix>>>
<http://lvestats.deepmetrix.com/stats?type=loginverid=deepmetrix&username=guest>

In the "Tabular – Who's On – XX Active Visitors" area of the "Who's On" page, expand the IP address that fetched. The next window will include the alert() popup.

Vendor status:

The vendor was notified on the 17th of May 2002.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:security@satus.com>> Daniel Bowers.

=====

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: "[REVS] Bypassing JavaScript Filters – the Flash! Attack"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)