

# [NT] Websense Blocked Sites XSS

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0018.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 12/04/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 4 Dec 2003 14:29:47 +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>

-----

Websense Blocked Sites XSS

---

## SUMMARY

When <http://www.websense.com> Websense blocks a web site, it returns a web page to the browser stating that the site has been blocked. This error message contains the URL which was requested. Websense does not do any validation or encoding of the URL before returning it in the error message. This allows an attacker to supply a URL that contains JavaScript, ActiveX, VB, etc). This script will run in the context of a server in the trusted domain and combined with other IE flaws can have serious consequences.

## DETAILS

Vulnerable systems:

\* Websense Enterprise version 4.3.0 up to version 5.1

Example:

A URL like: [http://BlockedSite?<SCRIPT>alert\('hello'\)</SCRIPT>](http://BlockedSite?<SCRIPT>alert('hello')</SCRIPT>) can be used to demonstrate the issue.

Resolution:

The vendor has come out with a patch (The vendor was notified on Nov 29, 2003).

Securiteam: [NT] Websense Blocked Sites XSS

ADDITIONAL INFORMATION

The information has been provided by <mailto:petert@imagine-sw.com> Mr. P.Taylor.

=====

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.