

[NT] WebWasher Classic Error Message XSS Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-11/0059.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/16/03

To: list@securiteam.com

Date: 16 Nov 2003 18:45:32 +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>

WebWasher Classic Error Message XSS Vulnerability

SUMMARY

<http://www.webwasher.com/client/home/index.html?lang=de_EN> WebWasher Classic, is WebWasher's easy-to-use and very effective Internet filter and assistant which runs on the client, a vulnerability in the product allows attackers to cause the product to return arbitrary HTML and/or JavaScript.

DETAILS

Vulnerable systems:

* WebWasher version 3.3 Build 44

* WebWasher version 2.2.1

WebWasher Classic is vulnerable to a XSS attack. If a HTTP GET-Request, containing script code, is sent to the proxy port (default 8080/TCP), an error page is shown, which contains the requested URL in the message body.

Thereby no validation of the requested URL, regarding script code, is done. It should be mentioned that if WebWasher proxy runs in server mode, the proxy port is accessible from the network. If WebWasher proxy runs in client mode, only connections from localhost are possible.

Securiteam: [NT] WebWasher Classic Error Message XSS Vulnerability

Example:

[http://localhost:8080/<script>alert\("WASH_ME"\)</script>](http://localhost:8080/<script>alert()

ADDITIONAL INFORMATION

The information has been provided by <mailto:Oliver.Karow@gmx.de> Oliver Karow.

=====

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.