

# [NEWS] Various Problems in Baltimore's WEBSweeper Script Filtering

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2001-08/0064.html>

---

*From:* [support@securiteam.com](mailto:support@securiteam.com)

*Date:* 08/15/01

From: [support@securiteam.com](mailto:support@securiteam.com)

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

Subject: [NEWS] Various Problems in Baltimore's WEBSweeper Script Filtering

Message-Id: <20010815065219.4FC44138BF@mail.der-keiler.de>

Date: Wed, 15 Aug 2001 08:52:19 +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>

## Various Problems in Baltimore's WEBSweeper Script Filtering

---

### SUMMARY

<<http://www.mimesweeper.com/products/websweeper4/default.asp>> WEBSweeper, a product that enables customers to implement Content Security policies on Web, HTTP and passive FTP transfers, has been found to contain a security vulnerability that allows attackers to execute arbitrary JavaScript on clients protected by WEBSweeper, bypassing the product's filtering mechanism.

### DETAILS

Vulnerable systems:

Baltimore Technologies WEBSweeper 4.02

WEBSweeper includes some design and implementation flaws that allow an attacker to bypass restrictions set by the product administrator and introduce malicious code into an organization.

eDvice found three problems with WEBSweeper's Script filtering mechanism:

1) By adding an extra opening angled bracket before the SCRIPT tag, the tag will be left unmodified by WEBSweeper. The browser however, will execute the contained script. Example:

```
<<SCRIPT language="javascript">  
alert("This should have been filtered");
```

Securiteam: [NEWS] Various Problems in Baltimore's WEBSweeper S

</SCRIPT>

2) Similar problem to the one eDvice reported in <<http://www.securiteam.com/securitynews/5EP0W0A4AO.html>> eSafe Gateway Bypassing Using Extended Character Encoding, WEBSweeper appears to manifest the same problem. The following designed HTML code:

```
<SC<SCRIPT language="javascript"> </SCRIPT>RIPT language="javascript">
alert("This should have been filtered");
</SCRIPT>
```

Will be transformed by the WEBSweeper filter to yield the following result:

```
<SCRIPT language="javascript">
alert("This should have been filtered");
</SCRIPT>
```

3) WEBSweeper does not recognize and does not filter scripting tags constructed using extended HTML notation.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:support@edvicesecurity.com>> eDvice Security Services.

=====

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](mailto:list-unsubscribe@securiteam.com) In order to subscribe to the mailing list, simply forward this email to: [list-subscribe@securiteam.com](mailto: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](mailto:support@securiteam.com): "[NT] Sambar Telnet Proxy Multiple Vulnerabilities (DoS, Buffer Overflow)"
  - **Messages sorted by:** [\[ date \]](#) [\[ thread \]](#) [\[ subject \]](#) [\[ author \]](#) [\[ attachment \]](#)