

CSS found in Movable Type

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-05/0125.html>

From: DarkHunter (darkhunter7_at_hackermail.com)

Date: 05/12/03

Date: 12 May 2003 18:26:59 -0000

To: bugtraq@securityfocus.com

('binary' encoding is not supported, stored as-is)

Summary:

Movable Type is a decentralized web-based personal publishing system designed to ease maintenance of regularly-updated content. This content can consist of, but is not limited to, entries in a weblog or online journal, photographs in an online photo gallery, news headlines on a newspaper site, or articles in an online magazine.

Details:

Vendor's site: www.movabletype.org

Vulnerable systems:

Movable Type version 2.63 and prior.

Cross Site Scripting Vulnerability found in writing the comments, in the Comments section there is several textboxes:

Name, Email Address, URL and Comments.

and all the textboxes allow using the javascript codes.

in order to causes a CSS attack on the target site we need to write a javascript code in the Name textbox (in some versions u can write the javascript code in the other textboxes of the Comments).

Examples:

You can use this javascripts codes:

```
&lt;script&gt;alert(document.cookie)&lt;/script&gt;
```

```
&lt;script&gt;alert("CSS discovered by DarkHunter")&lt;/script&gt;
```

```
"DarkHunter"&lt;script&gt; .. (This code is so bad :) .. it causes disappearing of all the Comments textboxes and buttons .. in other words every thing after this code will disappear).
```

and of course there are many codes that u can use.

Solution:

Edit the source code to strip malicious characters from Name, Email Address, URL and Comments textboxes or escape malicious characters using `addslashes()`.

SecurityFocus Bugtraq: CSS found in Movable Type

check the vendor's website for new patches.

Additional information:

The information has been provided by DarkHunter.