

[NEWS] Microsoft Hotmail Cross-Site Scripting (XSS) Flaws

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0074.html>

From: support@securiteam.com

Date: 12/22/02

From: support@securiteam.com

To: list@securiteam.com

Date: 22 Dec 2002 12:11:46 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Microsoft Hotmail Cross-Site Scripting (XSS) Flaws

SUMMARY

<<http://www.hotmail.com>> Hotmail is the world's largest provider of free, Web-based e-mail. It is based on the premise that e-mail access should be easy and possible from any computer connected to the World Wide Web. Hotmail eliminates the disparities among e-mail programs by adhering to the universal Hypertext Transfer Protocol (HTTP) standard. A cross site scripting vulnerability in the web site allows remote attackers to cause a user to execute arbitrary code.

DETAILS

The susceptibility of Microsoft Corp.'s MSN Hotmail to two cross-site scripting (XSS) attacks could allow attackers to infiltrate a targeted Hotmail user's e-mail account. Both attacks stem from incorrect or incomplete HTML filtering by Hotmail.

Issue One: Session Hijacking

While Hotmail does filter a number of HTML tags, it fails to filter the <textarea> tag. As such, an attacker could trick the Hotmail parser into treating a </textarea> tag as part of the literal value of a <td> background variable. Since the <textarea> tag does not rely on quotes and

Securiteam: [NEWS] Microsoft Hotmail Cross-Site Scripting (XSS) Flaws

ends when it reaches a closing `</textarea>` tag, the attacker could insert a JavaScript routine that would not be filtered.

The inserted routine could not contain any quotes, as Hotmail filters out such characters. This, however, could be overcome by using the `String.fromCharCode()` method, which converts an ASCII value to a string.

Issue Two: Arbitrary Action Execution

Hotmail does filter a number of variables, but it fails to filter the `<td>` background variable. Knowing this, an attacker could dupe a targeted user into opening an HTML-enabled e-mail to generate a GET request on a Hotmail server to execute an action. For example, Hotmail has filters in place that replace the following HTML:

```
<td width=1 height=1 bgcolor=\  
background='http://hotmail.msn.com/cgi-bin/dofolders?m=&i=&FID_=&from=inbox&newfoldername=HACKED'>/td>
```

Hotmail does not properly filter URLs that are composed with

The HTML above is replaced with the following:

```
<td width=1 height=1 bgcolor=~  
background='http://64.4.14.24/spacer.gif'></td>
```

However, Hotmail does not properly filter URLs that are composed with backslashes. So the following HTML would filter incorrectly:

```
<td width=1 height=1 bgcolor=\  
background='http://hotmail.msn.com\cgi-bin\dofolders?m=&i=&FID_=&from=inbox&newfoldername=HACKED'>/td>
```

The HTML above becomes:

```
<TD width=1 height=1 bgcolor=~  
background='http://hotmail.msn.com\cgi-bin\dofolders?m=&i=&FID_=&from=inbox&newfoldername=HACKED'></TD>
```

When the page loads, the code would generate a GET request to the specified URL. The URL is in the Hotmail domain, thus the user's cookie would transmit with the request. The Hotmail server would process the request and create a folder named HACKED.

Analysis:

Unlike most XSS attacks, which require a user to click on a tainted link, exploitation in this case only requires a Hotmail user to view a malicious e-mail. Sending the e-mail from a forged e-mail address affords a greater chance for successful exploitation. Once an attacker compromises one Hotmail user's account, the attacker could then use that account to compromise other e-mail accounts.

It is quite feasible for an automated worm to be written in such a way that it spreads through the enumeration of user address books. Such a worm would quickly propagate as future attack e-mails would arrive from known and trusted e-mail addresses.

Once a user's Hotmail cookie has been stolen, an attacker has the ability to gain full control over the user's account until the user logs out or

Securiteam: [NEWS] Microsoft Hotmail Cross-Site Scripting (XSS) Flaws

the session times out. (Hotmail's default setting is to never timeout). During that time, an attacker could read, remove, and store all e-mails, as well as send e-mails from the compromised account.

The ability to execute arbitrary Hotmail actions allows an attacker to set any option that the targeted user could normally set under the Options menu. This includes redirecting all e-mail to the deleted folder and modifying the user's name or e-mail signature.

For further information on this class of attacks, refer to "The Evolution of Cross-Site Scripting Attacks," an iDEFENSE White Paper available at <http://www.odefense.com/papers.html>

Detection:

All Hotmail users were vulnerable to the above described attacks before Microsoft resolved the issues.

Vendor fix:

Microsoft fixed this issue in hotmail on 11/04/2002.

Disclosure timeline:

10/08/2002 Issue disclosed to iDEFENSE
10/31/2002 Issue disclosed to Microsoft (secure@microsoft.com)
10/31/2002 Response received from secure@microsoft.com (Terri Forslof)
11/01/2002 iDEFENSE Clients notified
11/05/2002 Response received from secure@microsoft.com indicating issue was resolved at 3:00pm PST 11/04/2002
12/20/2002 Public Disclosure

ADDITIONAL INFORMATION

The original advisory can be downloaded by going to:

<http://www.odefense.com/advisory/12.20.02.txt>
<http://www.odefense.com/advisory/12.20.02.txt>

The information has been provided by <mailto:listserv@odefense.com>

iDEFENSE Labs, the vulnerability was discovered by

<mailto:David@cgishield.com> David Zentner.

=====

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.

Securiteam: [NEWS] Microsoft Hotmail Cross–Site Scripting (XSS) Flaws

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.