

[NEWS] Hotmail Cross-Site Scripting Vulnerability (IE gte)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-12/0061.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/20/04

To: list@securiteam.com

Date: 20 Dec 2004 18:34:30 +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>

Hotmail Cross-Site Scripting Vulnerability (IE gte)

SUMMARY

Finjan has discovered a script injection vulnerability in Hotmail that allows a remote attacker to execute malicious scripts when the victim is reading his/her mail, this vulnerability exploits Hotmail's in ability to properly detect JavaScript "protected" by an Internet Explorer internal proprietary tag parser (<! [if IE gte 4]>).

DETAILS

Hotmail's mobile code filtering mechanism is based on an active content filter whose purpose is to block the injection of any active content into Hotmail messages. Hotmail's filter identifies any possibly malicious HTML tags, properties and elements, and then modifies them into a non-malicious code.

When analyzing an HTML condition comment tag (for example: < ![if IE gte 4]>), Hotmail's filter changes it to a comment (e.g. < ![if IE gte 4]>). A space character is added after the ! , making the code inside the condition be treated as a comment rather than as an executable. Any potentially malicious code inside the condition is not altered.

Securiteam: [NEWS] Hotmail Cross-Site Scripting Vulnerability (IE gte)

For example:

```
< ![if IE gte 4]>< style>@\im\port\ja\vasc\ript>alert();</style>
```

In order to bypass this protection, a comment tag can be added before the condition tag.

For example:

```
< !-- <![if IE gte 4]>< style>@\im\port\ja\vasc\ript>alert();</style>
```

At this stage the code is harmless since Internet browsers treat this script as an HTML comment. However, a possible risk arises when an HTML condition comment tag opener (<!) is inserted at the beginning of the code.

For example:

```
< ! <!-- <![if IE gte 4]>< style>@\im\port\ja\vasc\ript>alert();</style>
```

Since Hotmail's HTML filter treats this code as a comment, it does not filter out the script. In contrast, Internet browsers do not treat this script as a comment, but rather execute the code inside the condition tag. In this manner, any tag that supports style, events or JavaScript execution can be used to remotely call a JavaScript file.

The injected JavaScript code could be used for:

- * Automatically launching malicious code
- * Stealing the victim s password by using a spoofed re-login window
- * Reading the victim s INBOX and contacts
- * Sending email messages without any user authorization

Proof of Concept:

```
< !  
<!--  
< ![if IE gte 4]>< style>@\im\port\ja\vasc\ript>alert();</style>
```

Vulnerability Status

Vendor was notified on Sep 8th, 2004. The bug is now fixed.

ADDITIONAL INFORMATION

The information has been provided by <mailto:theinsider@012.net.il> Rafel Ivgi, The-Insider.

=====

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.