

[VulnWatch] Simple Yahoo! Mail Cross-Site Scripting (GM#006-MC)

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-06/0004.html>

From: GreyMagic Software (*security_at_greymagic.com*)

Date: 06/03/04

To: <vulnwatch@vulnwatch.org>

Date: Thu, 3 Jun 2004 15:52:32 +0200

GreyMagic Security Advisory GM#006-MC
=====

GreyMagic Software, 03 Jun 2004.

Available in HTML format at

<http://www.greymagic.com/security/advisories/gm006-mc/>.

Topic: Simple Yahoo! Mail Cross-Site Scripting.

Discovery date: 16 May 2004.

Affected applications:
=====

* Yahoo! web-based email service.

Introduction:
=====

Web-based email services and Yahoo! specifically make tremendous efforts to sanitize incoming emails from potentially unsafe HTML content. Flawed filtering of such unsafe content may result in severe consequences that would occur as soon as a user opens an email for reading, including:

- * Theft of login and password.
- * Content disclosure of any email in the mailbox.
- * Automatically send emails from the mailbox.
- * Exploitation of known vulnerabilities in the browser to access the user's file system and eventually take over the machine.
- * Distribution of a web-based email worm.
- * Disclosure of all contacts within the address book.

Discussion:
=====

VulnWatch: [VulnWatch] Simple Yahoo! Mail Cross-Site Scripting (GM#006-MC)

GreyMagic discovered that by sending a maliciously formed email to a Yahoo user it is possible to circumvent the filter and execute script in the context of a logged-in Yahoo! user.

A known Cross-Site Scripting weakness is using entities instead of actual chars, for example: "javascript:alert()". There is also a variation of that weakness, caused by the way browsers ignore white-space chars in URLs: "javascript:alert()". Yahoo! properly filters both of these scenarios.

However, a third variation remains unfiltered. It is possible to embed a javascript URL by using a white-space entity with multiple zero chars in front of it: "javascript:alert()".

Exploit:

=====

The following HTML embedded in an email would show a Yahoo! user's cookie when opened:

```
<div
style="background-image:url(jav&#000013;ascript:alert(document.cookie))">Hello!</div>
```

Solution:

=====

GreyMagic informed Yahoo! of the vulnerability on 20-May-2004. Yahoo! responded promptly and reported that it patched the vulnerability on 24-May-2004.

Tested on:

=====

Yahoo! web-based email service.

Disclaimer:

=====

The information in this advisory and any of its demonstrations is provided "as is" without warranty of any kind.

GreyMagic Software is not liable for any direct or indirect damages caused as a result of using the information or demonstrations provided in any part of this advisory.

– Copyright © 2004 GreyMagic Software.