

[NT] Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack (MS03-047)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0075.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/19/03

To: list@securiteam.com

Date: 19 Oct 2003 12:12:03 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

The SecuriTeam alerts list - Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.secureteam.com/maillinglist.html>

Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack (MS03-047)

SUMMARY

A cross-site scripting (XSS) vulnerability results due to the way that Outlook Web Access (OWA) performs HTML encoding in the Compose New Message form.

DETAILS

Vulnerable Systems:

- * Microsoft Exchange Server 5.5, Service Pack 4

Immune Systems:

- * Microsoft Exchange 2000 Server
- * Microsoft Exchange Server 2003

Patch Availability:

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C516FE75-95CE-4FFF-B83D-9B170FCD0C1C&dis>>
Microsoft Exchange Server 5.5, Service Pack 4

[NT] Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting Attack (MS03-047)

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0712>>
CAN-2003-0712

An attacker could seek to exploit this vulnerability by having a user run script on the attacker's behalf. The script would execute in the security context of the user. If the script executes in the security context of the user, the attacker's code could then execute by using the security settings of the OWA Web site (or of a Web site that is hosted on the same server as the OWA Web site) and could enable the attacker to access any data belonging to the site where the user has access.

To exploit this vulnerability through OWA, an attacker would have to send an e-mail message that has a specially-formed link to the user. The user would then have to click the link. To exploit this vulnerability in another way, an attacker would have to know the name of the user's Exchange server and then entice the user to open a specially-formed link from another source while the user is logged on to OWA.

Note: Customers who have customized any of the ASP pages in the File Information section in this document should backup those files before applying this patch as they will be overwritten when the patch is applied. Any customizations would then need to be reapplied to the new ASP pages. Please refer to the Microsoft Support Policy for the Customization of Outlook Web Access available at

<<http://support.microsoft.com/default.aspx?scid=kb:en-us:327178>>
<http://support.microsoft.com/default.aspx?scid=kb:en-us:327178>

Mitigating factors:

* To be affected, the user would have to be logged onto OWA, be enticed to log on to OWA, or use another Web application on the same server as OWA. Generally, a server that runs Exchange Server 5.5 Outlook Web Access does not run other Web applications for reasons of performance, scalability, and security.

* To exploit this vulnerability through OWA, an attacker would have to send an e-mail message that has a specially-formed link to a user. The user would then have to click the link.

* In the Web-based attack vector, an attacker would have to know the name of a user's Exchange server and then entice the user to open a specially-formed link from some other source while the user is logged on to OWA.

Workarounds

Microsoft has tested the following workarounds. These workarounds will not correct the underlying vulnerability however they help block known attack vectors. Workarounds may cause a reduction in functionality in some cases. In such situations this is identified below.

* Disable Outlook Web Access for each Exchange site

Outlook Web Access can be disabled by following these steps. These steps need to be performed on each Exchange site.

1. Start Exchange Administrator
2. Expand the Configuration container for the site.
3. Select the Protocols container for the site.

4. Open the properties of the HTTP (Web) Site Settings object
5. Clear the "Enable Protocol" checkbox.
6. Wait for the change to replicate, and then verify that this change has replicated to each server in the site. To do this, bind to each server in the site with Exchange Administrator and view the setting.

Impact of Workaround:

Users will have no access to their mailboxes via Outlook Web Access.

* Uninstall Outlook Web Access

For steps on how to do this please refer to the Knowledge Base Article "<http://support.microsoft.com/default.aspx?scid=kb:en-us:290287>> How to Completely Remove and Re-Install OWA"

Impact of Workaround: Users will have no access to their mailboxes via Outlook Web Access.

For additional information about how to help make your Exchange environment more secure, visit the Security Resources for Exchange 5.5 Web site.

Frequently Asked Questions

What is the scope of this vulnerability?

This is a cross-site scripting vulnerability. This vulnerability could enable an attacker to cause arbitrary code to run during another user's Web session. The code could take any action on the user's computer that the Web site is authorized to take; this could include monitoring the Web session and forwarding information to a third party, running other code on the user's system and reading or writing cookies. The code could be written to be persistent, so that if the user returned to the Web site again, the code would run again.

The vulnerability cannot be "injected" into a Web session; it can only be exploited if the user clicks a hyperlink that the attacker provides.

To exploit this vulnerability in another way, other than sending the specially formed link in email to a user, an attacker would have to know the name of a user's Exchange server and then entice the user to open a specially-formed link from some other source while the user is logged on to OWA.

What is Outlook Web Access?

Microsoft Outlook Web Access (OWA) is a service of Exchange Server. By using OWA, users can use a Web browser to access their Exchange mailbox. By using OWA, a server that is running Exchange Server can also function as a Web site that lets authorized users read or send mail, manage their calendar, or perform other mail functions over the Internet.

What is cross-site scripting?

Cross-site scripting (XSS) is a security vulnerability that could enable an attacker to "inject" code into a user's session with a Web site. Unlike most security vulnerabilities, XSS does not apply to any single vendor's products – instead, it can affect any software that generates HTML and that does not follow defensive programming practices.

How does XSS work?

Web pages contain text and HTML markup, which are generated by the server and are interpreted by the client. Servers that generate static pages have full control over the way that the client interprets the pages that the server sends. However, servers that generate dynamic pages do not have control over the way that the client interprets their output. If untrusted content can be introduced into a dynamic page, neither the server nor the client has sufficient information to recognize that this has occurred and to take protective actions.

More information about how cross-site scripting works and what can be done to mitigate such attacks can be found at

<<http://www.microsoft.com/technet/security/news/crssite.asp>> Information about Cross-Site Scripting Security Vulnerability.

What causes the vulnerability?

The vulnerability results because the Active Server Page (ASP) that Exchange Server 5.5 Outlook Web Access uses when it composes new messages replays the requested URL in HTML without the correct encoding.

What is wrong with Outlook Web Access?

When a user creates a new e-mail message, OWA does not correctly encode the URL for display in HTML. As a result, an attacker could embed a link to a script on a separate Web site and could cause the link to be returned to the Web browser in such a way that the browser thinks that it comes from the OWA Web site.

What could this vulnerability enable an attacker to do?

The vulnerability could enable an attacker who hosts a malicious Web site, or who can entice a user to click a specially-formed link, to carry out a cross-site scripting attack against the user's OWA Web site. By doing so, an attacker could run script in the user's browser and could use the security settings of the OWA Web site or any other Web site that is hosted on the same system and to could access cookies and other data that belong to the Web site.

How could an attacker exploit this vulnerability?

An attacker who hosts a malicious Web site could seek to exploit this vulnerability by sending a specially-crafted e-mail message that has an embedded script or link that, when accessed, would send out a Web server query that has a script as part of one of the arguments. The user would have to click the link in the e-mail message while it appears in OWA or while it appears on an external Web site.

Are all versions of OWA are vulnerable?

No. The vulnerability affects only Exchange Server 5.5 Outlook Web Access.

On which Exchange servers should I install the patch?

This patch is intended only for servers that are running Exchange Server 5.5 Outlook Web Access. You do not have to install this patch on servers that are not running Exchange Server 5.5 Outlook Web Access.

I have customized my OWA site, what do I do?

Customers having customized any of the ASP pages in the File Information section in this document should backup those files before applying this patch as they will be overwritten when the patch is applied. Any customizations would then need to be reapplied to the new ASP pages. Please refer to the Microsoft Support Policy for the Customization of Outlook Web Access available at

<http://support.microsoft.com/default.aspx?scid=kb:en-us:327178>
<http://support.microsoft.com/default.aspx?scid=kb:en-us:327178>

How does the patch eliminate the vulnerability?

The patch eliminates the vulnerability by ensuring that OWA script arguments are encoded so that they cannot be unintentionally executed.

Microsoft thanks the following for working with us to protect customers:
Ory Segal of Sanctum Inc. for reporting the issue described in MS03-047.

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/MS03-047.asp>
<http://www.microsoft.com/technet/security/bulletin/MS03-047.asp>

=====

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.