

[NT] Vulnerability in Outlook Web Access for Exchange Server 5.5 Allows XSS (MS05-029)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-06/0052.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/15/05

To: list@securiteam.com

Date: 15 Jun 2005 10:16:10 +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>

Vulnerability in Outlook Web Access for Exchange Server 5.5 Allows XSS
(MS05-029)

SUMMARY

A cross-site scripting vulnerability has been found in Outlook Web Access that is provided by Exchange Server 5.5. The cross-site scripting vulnerability allows an attacker to convince a user to run a malicious script. If this malicious script is run, it would execute in the security context of the user. Attempts to exploit this vulnerability require user interaction. This vulnerability could allow an attacker access to any data on the Outlook Web Access server that was accessible to the individual user.

DETAILS

Affected Software:

Microsoft Exchange Server 5.5 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?familyid=08435B77-9F3A-40F5-B13A-A7019CB1C244>>

Download the update

Non-Affected Software:

* Microsoft Exchange 2000 Server Service Pack 3 with the Exchange 2000

Securiteam: [NT] Vulnerability in Outlook Web Access for Exchange Server 5.5 Allows XSS (MS05-029)

Post-Service Pack 3 Update Rollup of August 2004.

- * Microsoft Exchange Server 2003

- * Microsoft Exchange Server 2003 Service Pack 1

CVE Information:

Exchange Server Outlook Web Access Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0563>>

CAN-2005-0563

Mitigating Factors for Exchange Server Outlook Web Access Vulnerability –

CAN-2005-0563:

- * To be affected, the user would have to be logged onto Outlook Web Access (OWA).

- * The following supported versions of Outlook Web Access for Exchange Server are not affected

- * Outlook Web Access for Exchange 2000 Server Exchange 2000 Post-Service Pack 3 Update Rollup of August 2004.

- * Outlook Web Access for Exchange Server 2003

- * Outlook Web Access for Exchange Server 2003 Service Pack 1

Workarounds for Exchange Server Outlook Web Access Vulnerability –

CAN-2005-0563:

Microsoft has tested the following workarounds. While these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

Modify the Read.asp file

To modify the Read.asp file, follow these steps.

Note Administrators can modify the Read.asp file.

Note These steps must be performed on each Outlook Web Access server.

1. Open the Read.asp file in Notepad. This file is located in the following folder: C:\Exchsrvr\Webdata\

2. Locate the following line of code: <%= bstrBody %>

3. Save the file.

4. Change that line of code to the following:

Changes will take effect immediately.

Impact of workaround:

E-mail that is formatted in HTML will not display correctly. Users will see the raw HTML behind the e-mail.

Disable Outlook Web Access for each Exchange site

To disable Outlook Web Access follow these steps.

Note These steps must 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 the change has replicated to each server in the site. To do this, bind to each server in

Securiteam: [NT] Vulnerability in Outlook Web Access for Exchange Server 5.5 Allows XSS (MS05-029)

the site by using Exchange Administrator, and then view the Enabled Protocol check box setting.

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

Uninstall Outlook Web Access

For information about how to uninstall Outlook Web Access, see Microsoft <<http://support.microsoft.com/default.aspx?scid=kb;en-us;290287>> Knowledge Base Article 290287.

Impact of Workaround:

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

For more information about how to help make your Exchange environment more secure, visit the

<<http://www.microsoft.com/technet/prodtechnol/exchange/55/maintain/secure.msp>> Security Resources for Exchange 5.5 Web site.

FAQ for Exchange Server Outlook Web Access Vulnerability – CAN-2005-0563:

What is the scope of the vulnerability?

This is a cross-site scripting vulnerability that could allow an attacker to convince a user to run a malicious script. If this malicious script is run, it would execute in the security context of the user. Attempts to exploit this vulnerability require user interaction.

The script 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.

What is Outlook Web Access?

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

What causes the vulnerability?

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

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 cross-site scripting work?

Web pages contain text and HTML markup. Text and HTML markup 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

Securiteam: [NT] Vulnerability in Outlook Web Access for Exchange Server 5.5 Allows XSS (MS05-029)

pages that the server sends. However, servers that generate dynamic pages do not have control over the way that the client interprets the servers output. If untrusted content is introduced into a dynamic page, neither the server nor the client has sufficient information to recognize that this action has occurred and to take protective measures.

How could an attacker exploit the vulnerability?

An attacker could try to exploit this vulnerability by sending a specially crafted message to a user. The user would then have to open the message by using Outlook Web Access. The message could then cause the affected system to run script in the context of the user's Outlook Web Access session.

What systems are primarily at risk from the vulnerability?

Client systems accessing an Exchange Server 5.5 through Outlook Web Access are primarily at risk from this vulnerability.

Are all supported versions of Outlook Web Access vulnerable?

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

On which Exchange servers should I install the update?

This update is intended only for servers that are running Outlook Web Access for Exchange Server 5.5. You do not have to install this update on servers that are not running Outlook Web Access for Exchange Server 5.5. However, we recommend that you install this security update on all other servers running Exchange 5.5 servers to help protect them if they are later designated as Outlook Web Access servers.

What does the update do?

The update removes the vulnerability by making sure that OWA script arguments are encoded so that they cannot be unintentionally executed.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms05-029.mspx>
<http://www.microsoft.com/technet/security/bulletin/ms05-029.mspx>

=====

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.