

[NT] Microsoft Exchange Server Outlook Web Access Script Injection (MS06-029)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-06/msg00043.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 14 Jun 2006 12:24:21 +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>

Microsoft Exchange Server Outlook Web Access Script Injection (MS06-029)

SUMMARY

A script injection vulnerability exists in Exchange Server running Outlook Web Access (OWA). An attacker could exploit the vulnerability by constructing an e-mail message with a specially crafted script. If this specially crafted script is run, it would execute in the security context of the user on the client. Attempts to exploit this vulnerability require user interaction.

Vulnerability in Microsoft Exchange Server running Outlook Web Access could allow script injection.

DETAILS

Vulnerable Systems:

* Microsoft Exchange 2000 Server Pack 3 with the August 2004 Exchange 2000 Server Post-Service Pack 3 Update Rollup –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=746CE64E-3186-422B-A13B-004E7942189B>>

Download the update (KB912442)

* Microsoft Exchange Server 2003 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0E192781-847F-41C1-B32A-84218DB60942>>

[NT] Microsoft Exchange Server Outlook Web Access Script Injection (MS06-029)

Download the update (KB912442)

* Microsoft Exchange Server 2003 Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=C777BC9F-52B7-4F17-96C7-DAF3B9987D70>>

Download the update (KB912442)

Mitigations for Microsoft Exchange Server When Running Outlook Web Access

Vulnerability:

* To be affected, a user would have to use Outlook Web Access to read a specially crafted e-mail message.

Workarounds for Microsoft Exchange Server When Running Outlook Web Access

Vulnerability:

Microsoft has tested the following workarounds. Although 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.

* Disable Outlook Web Access (OWA) on a computer running Exchange Server

Disabling Outlook Web Access helps protect the affected system from attempts to exploit this vulnerability. To disable Outlook Web Access, follow these steps:

1. Click Start, point to All Programs, point to Microsoft Exchange, and then click System Manager.
2. Expand Servers, expand Server, expand Protocols, and then expand HTTP.
3. Right-click Exchange Virtual Server, and then click Stop.

Note A red cross will appear over the Exchange Virtual Server icon, indicating it has been stopped. From now on, users will see a The Page Cannot Be Displayed error message when they try to access their e-mail through OWA.

Impact of Workaround: This workaround prevents users from accessing their mailboxes through Outlook Web Access (OWA), Outlook Mobile Access (OMA) and Exchange Server ActiveSync.

FAQ for Microsoft Exchange Server When Running Outlook Web Access

Vulnerability:

What is the scope of the vulnerability?

A script injection vulnerability exists that could allow an attacker to run a malicious script. If this malicious script is run, it would run in the security context of the user on the client. The script could take any action on the user's computer that the Web site is authorized to take. These actions could include monitoring the user's 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?

[NT] Microsoft Exchange Server Outlook Web Access Script Injection (MS06-029)

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 e-mail, manage their calendar, and perform other e-mail functions over the Internet.

What causes the vulnerability?

This vulnerability is caused by the way that Outlook Web Access incorrectly filtering script under certain circumstances within an e-mail message.

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 users are primarily at risk from the vulnerability?

Users who are using Microsoft Exchange Outlook Web Access to read e-mail are primarily at risk.

What does the update do?

The update removes the vulnerability by modifying the way that Outlook Web Access handles HTML parsing.

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.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-1193>>
CVE-2006-1193

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms06-029.mspx>>
<http://www.microsoft.com/technet/security/bulletin/ms06-029.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@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

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.