

[NT] Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0048.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/14/04

To: list@securiteam.com

Date: 14 Jan 2004 11:46:22 +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 Exchange Server 2003 Could Lead to Privilege Escalation
(MS04-002)

SUMMARY

A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing OWA access and, when running Outlook Web Access (OWA) on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003.

Users who access their mailboxes through an Exchange 2003 front-end server and Outlook Web Access might be connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA.

By default, Kerberos authentication is used as the HTTP authentication method between Exchange Server 2003 front-end and back-end Exchange servers. This behavior manifests itself only in deployments where OWA is

Securiteam: [NT] Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002)

used in an Exchange front-end/back-end server configuration and Kerberos has been disabled as an authentication method for OWA communication between the front-end and back-end Exchange servers.

This vulnerability is exposed if the Web site that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. This vulnerability cannot be exposed by a routine fallback to NTLM because of a problem with Kerberos authentication. This configuration change may occur when Microsoft Windows SharePoint Services (WSS) 2.0 is installed on a Windows Server 2003 server that also functions as an Exchange Server 2003 back-end.

DETAILS

Affected Software:

- * Microsoft Exchange Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=9542F949-D09B-4199-A837-FBCFC0567676&disp>

Download the update

Non Affected Software:

- * Microsoft Exchange 2000 Server
- * Microsoft Exchange Server 5.5

Mitigating factors:

- * To exploit this vulnerability, an attacker would first have to authenticate to an Exchange Server 2003 front-end server.
- * The mailbox that an attacker could get access to is random and not possible to predict. It is also not that they would be connected to another user's mailbox at all.
- * Only mailboxes that have recently been accessed through Outlook Web Access using the same pair of front-end and back-end servers could be affected.
- * Exchange 2000 Server and Exchange Server 5.5 are not affected by this vulnerability.
- * Only deployments that have a front-end server that hosts Outlook Web Access for Exchange 2003 Server, that runs on either Windows 2000 or Windows Server 2003, and that has a back-end Exchange Server 2003 that runs on Windows Server 2003 are affected by this vulnerability.
- * By default, Kerberos authentication is used for HTTP requests between an Exchange Server 2003 front-end server and an Exchange back end-server. This vulnerability is only exposed if the Web site that is running the Exchange Server 2003 programs on the Exchange back end-server has been configured not to negotiate Kerberos authentication, causing OWA to use NTLM authentication. This configuration change may occur when Microsoft Windows SharePoint Services is installed on a Windows Server 2003 server that also functions as an Exchange Server 2003 back-end.

Workarounds:

Microsoft has tested the following workarounds that apply to this vulnerability. These workarounds help block known attack vectors. However, they will not correct the underlying vulnerability. Workarounds may reduce functionality in some cases; in such cases, the reduction in functionality is identified below.

1. Disable HTTP connection reuse on an Exchange Server 2003 front-end server.

By default, Exchange Server 2003 reuses HTTP Connections between front-end and back-end servers to gain improved performance. Connection reuse can be turned off on the Exchange front-end server. Doing so could cause some performance degradation, but it is an effective workaround to this vulnerability. After you apply the update to the Exchange Server 2003 front-end server, you can remove this workaround.

See Microsoft Knowledge Base Article 832749 for information about how to disable HTTP connection reuse on a Microsoft Exchange Server 2003 front-end server.

Impact of workaround:

Clients may experience small performance degradation when they use OWA to access their mailboxes.

2. Enable Kerberos on the virtual server that hosts OWA on the Exchange Server 2003 back-end server.

The only known way that this vulnerability can be exposed is if Kerberos is disabled on the Internet Information Services virtual server where Outlook Web Access is hosted on the back-end server. This configuration change may occur when Windows SharePoint Services (WSS) 2.0 is installed on the same virtual server.

See Microsoft Knowledge Base Article 832769 for information about how to configure Windows SharePoint Services to use Kerberos authentication.

See Microsoft Knowledge Base Article 823265 for information about how to re-enable OWA and other Exchange components after you install Windows SharePoint Services.

Impact of workaround:

None

Frequently Asked Questions

What is the scope of the vulnerability?

Users who use Outlook Web Access for Exchange Server 2003 to access their mailboxes could connect to another user's mailbox. An attacker seeking to exploit this vulnerability could not predict which mailbox they would become connected to or if they would connect to another user's mailbox at all. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed

through OWA. This behavior occurs when OWA is used in an Exchange front-end server configuration and when Kerberos is disabled as an authentication method for the IIS Web site that hosts OWA on the back-end Exchange servers. By default, Kerberos authentication is used as the HTTP authentication method between Exchange Server 2003 front-end and back-end Exchange servers.

This vulnerability is only exposed if the Web site that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to use Kerberos authentication, and OWA is using NTLM authentication. This configuration change can occur when Microsoft Windows SharePoint Services is installed on a Windows Server 2003 server that also functions as an Exchange Server 2003 back-end.

What causes the vulnerability?

The vulnerability results because of the way that HTTP connections are reused when using NTLM authentication between Exchange 2003 front-end servers and Exchange 2003 back-end servers when the back-end server is running Windows Server 2003.

Even though Kerberos is enabled and used by default when an Exchange Server 2003 front-end component authenticates to the back-end Exchange server, there are situations when Kerberos authentication is explicitly disabled on the back-end server, and therefore only NTLM authentication is available.

What is Outlook Web Access?

Outlook Web Access is a feature 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 or send e-mail messages, manage their calendar, or perform other mail functions over the Internet by using a Web browser.

OWA can be deployed in an Exchange front-end/back-end server configuration.

What are front-end and back-end Exchange servers?

Exchange can be deployed so that end users with mailboxes on multiple servers can all connect to a single front-end Exchange server. This front-end server in turn connects ("proxies") to the appropriate back-end servers where mailboxes are actually stored.

What are Kerberos and NTLM?

Kerberos and NTLM are two different authentication protocols. Kerberos is the preferred Windows authentication protocol. It is used whenever possible and is the default protocol that Exchange Server 2003 uses between front-end and back-end Exchange servers for Outlook Web Access. NTLM authentication can be used as an alternate method when Kerberos authentication is unavailable.

How do I verify whether Kerberos is enabled for Outlook Web Access?

By default, Kerberos is enabled for OWA for Exchange Server 2003. However,

Securiteam: [NT] Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002)

because Internet Information Services is the Windows component that hosts OWA, check the configuration of your IIS server to verify that Kerberos is enabled. To verify the IIS authentication setting, look in the IIS metabase on the Exchange back-end server. To do so, use the following command-line commands:

```
* cscript.exe %SystemDrive%\inetpub\adminscripts\adsutil.vbs get w3svc/NTAuthenticationProviders
```

Alternatively,

```
* cscript.exe %SystemDrive%\inetpub\adminscripts\adsutil.vbs get w3svc/1/root/NTAuthenticationProviders
```

If only the value "NTLM" is returned, there may be a problem. The correct response is:

```
* "The parameter 'NTAuthenticationProviders' is not set at this node."
```

Alternatively,

```
* "Negotiate, NTLM"
```

The term negotiate is used to describe Kerberos authentication over HTTP.

See Microsoft Knowledge Base Article 832769 for information about how to configure Windows SharePoint Services to use Kerberos authentication.

I did not change any default security settings on my Exchange server. Is there any other way Kerberos might have been disabled on the Web site hosting the Exchange programs on the back-end Exchange server?

Yes. When a Microsoft Internet Information Services virtual server is extended with Windows SharePoint Services, the virtual server is subsequently configured to use Integrated Windows authentication (formerly named NTLM, or Windows NT Challenge/Response authentication) and explicitly disables Kerberos authentication. If Windows SharePoint Services (WSS) has been installed on the same server as an Exchange Server 2003 back-end running Windows Server 2003, Kerberos might have been disabled on the Web site hosting the Exchange programs.

See Microsoft Knowledge Base Article 832769 for information about how to configure Windows SharePoint Services to use Kerberos authentication.

See Microsoft Knowledge Base Article 823265 for information about how to re-enable OWA and other Exchange components after you install Windows SharePoint Services.

Who could exploit the vulnerability?

To exploit this vulnerability, an attacker would have to be an authorized user who has a mailbox on the same back-end Exchange server and who could first authenticate through OWA by using valid credentials.

Securiteam: [NT] Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002)

The mailbox that an attacker could access is random and cannot be predicted. It is also not certain that the attacker would get connected to another user's mailbox at all.

What could this vulnerability allow an attacker to do?

An authenticated user who gained access to another user's mailbox that is hosted on the same Exchange system could perform any action that the legitimate user could do through OWA. This includes reading, sending, and deleting e-mail messages in the user's mailbox.

What systems are primarily at risk from the vulnerability?

Only systems where Outlook Web Access is accessed through a Microsoft Exchange Server 2003 front end/back-end configuration are at risk from the vulnerability.

The back-end server must be running Exchange Server 2003 on Windows Server 2003. The front-end server can be running Windows 2000 or Windows Server 2003.

Can my OWA be affected although I do not have a front-end and back-end server configuration?

No. Exchange servers running OWA on the same server as the Exchange information store are not affected; only front-end/back-end Exchange Server 2003 configurations are affected by this vulnerability.

I am running Small Business Server 2003. Am I affected by this vulnerability?

No. Small Business Server is by default a single server setup with OWA access through the same server that hosts user mailboxes. Only front-end/back-end Exchange Server 2003 configurations are affected by this vulnerability.

Are all versions of Exchange and Outlook Web Access vulnerable?

No. The vulnerability affects only Outlook Web Access for Exchange Server 2003.

On which Exchange servers should I install the update?

This update is intended for front-end servers that are running Outlook Web Access for Microsoft Exchange Server 2003.

You do not have to install this update on back-end Exchange servers or on front-end Exchange servers that are not providing OWA services. However, it is recommended that you install this update on all systems that are running Exchange Server 2003 so that you are protected if you later migrate a back-end server to the role of a front-end server.

Does the update introduce any behavioral changes?

Yes. The update changes the connection pooling so that HTTP connections that use NTLM to authenticate are not added to the pool. It is unlikely that this behavioral change will be noticed by OWA end users.

Securiteam: [NT] Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation (MS04-002)

What does the update do?

The update removes the vulnerability by making sure that all authentication methods re-authenticate correctly before reusing any HTTP connections between the front-end and back-end Exchange servers, and that connections that are established by using NTLM authentication are not improperly reused.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

=====

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.