

[NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0074.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/19/03

To: list@securiteam.com

Date: 19 Oct 2003 12:08:36 +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 Could Allow Arbitrary Code Execution
(MS03-046)

SUMMARY

In Exchange Server 5.5, a security vulnerability exists in the Internet Mail Service that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted extended verb request that could allocate a large amount of memory. This could shut down the Internet Mail Service or could cause the server to stop responding because of a low memory condition.

DETAILS

Vulnerable Systems:

- * Microsoft Exchange Server 5.5, Service Pack 4
- * Microsoft Exchange 2000 Server, Service Pack 3

Immune Systems:

- * Microsoft Exchange Server 2003

Patch Availability:

*

Securiteam: [NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A9E872EA-54B0-4179-8AE9-5648BFB46459&disp>>
Microsoft Exchange Server 5.5, Service Pack 4

*

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=7BAF5394-1B4E-4937-A570-9F232AE49F01&disp>>
Microsoft Exchange 2000 Server, Service Pack 3

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0714>>
CAN-2003-0714

In Exchange 2000 Server, a security vulnerability exists that could allow an unauthenticated attacker to connect to the SMTP port on an Exchange server and issue a specially-crafted extended verb request. That request could cause a denial of service that is similar to the one that could occur on Exchange 5.5. Additionally, if an attacker issues the request with carefully chosen data, the attacker could cause a buffer overrun that could allow the attacker to run malicious programs of their choice in the security context of the SMTP service.

Mitigating Factors:

* Microsoft ISA Server 2000, or third-party products that relay and filter SMTP traffic before forwarding it to Exchange, could be used to prevent this attack over the Internet. Customers who use ISA Server 2000 to publish Exchange SMTP services with the default SMTP publishing rules are at reduced risk from this attack over the Internet. The Workarounds section below discusses these ISA publishing rules.

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 ?ç in such situations this is identified below.

* Use SMTP protocol inspection to filter out SMTP protocol extensions. There are default ISA publishing rules for Exchange for filtering out any SMTP protocol extensions from traffic that passes the firewall. Other third-party products may offer similar functionality. More information on how to publish an Exchange server computer with ISA Server can be found at:

<<http://support.microsoft.com/default.aspx?scid=kb;en-us:311237>>
<http://support.microsoft.com/default.aspx?scid=kb;en-us:311237>.

* Only accept authenticated SMTP sessions.

If practicle, accept only connections from SMTP servers that authenticate themselves by using the SMTP AUTH command.

To require SMTP authentication on an Exchange 2000 server:

1. Start Exchange System Manager.
2. Locate the server in the organization tree.
3. Expand the Protocols container for the server.
4. Expand the SMTP container.
5. For each SMTP virtual server:

Securiteam: [NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

- * Open the properties and of the virtual server object.
- * Click the Access properties page.
- * Click the Authentication button.
- * Clear the "Anonymous Access" checkbox.
- * Click OK to accept the change.

To require SMTP authentication on an Exchange 5.5 server:

To require authentication for inbound connections:

1. Click the Connections page.
2. In the "Accept Connections" Section, mark the radio button for "Only from hosts using Authentication."

Impact of Workaround:

Because most of the SMTP servers on the Internet only support Anonymous Authentication, inbound sessions from external SMTP servers will be affected.

Use a firewall to block the port that SMTP uses.

Use a firewall to block the port that SMTP uses. Typically, that is port 25.

Impact of Workaround : This workaround should only be used as a last resort to help protect you from this vulnerability. This workaround may directly affect the ability to communicate with external parties by e-mail.

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

<<http://www.microsoft.com/exchange/techinfo/security/55.asp>> Security Resources for Exchange 5.5 and

<<http://www.microsoft.com/exchange/techinfo/security/2000.asp>> Security Resources for Exchange 2000 Web sites.

Frequently Asked Questions

What is the scope of this vulnerability?

In Exchange Server 5.5, this is a denial of service vulnerability because an unauthenticated attacker could exhaust large amounts of memory on the server or could cause the Internet Mail Service to shut down. There is no buffer that is overrun in this version of Exchange.

In Exchange 2000 Server, this is a buffer overrun vulnerability that could allow an unauthenticated attacker to exhaust large amounts of memory on the server or, at worst, run arbitrary code of their choice on the affected system in the security context of the Local System account.

What causes the vulnerability?

In Exchange Server 5.5, an unauthenticated attacker could issue a specially crafted SMTP extended verb request to allocate large amounts of memory.

In Exchange 2000 Server, an unauthenticated attacker could issue a specially crafted SMTP extended verb request to exploit an unchecked buffer.

What is SMTP?

SMTP (Simple Mail Transfer Protocol) is an industry standard for delivering e-mail over the Internet, as defined in <http://www.ietf.org/rfc/rfc2821.txt?number=2821> and in <http://www.ietf.org/rfc/rfc2821.txt?number=2822>. The protocol defines the format of e-mail messages, the fields that are in e-mail messages, the contents of e-mail messages, and the handling procedures for e-mail messages.

What are SMTP extended verbs?

SMTP extended verbs are defined by the extension model that is defined in <http://www.ietf.org/rfc/rfc2821.txt?number=2821>. They allow addition of new functionality to the SMTP protocol. Microsoft Exchange uses an extended verb to communicate routing and other Exchange-specific information among Exchange servers in an Exchange environment.

What is wrong with the way that Exchange handles SMTP extended verbs? In Exchange Server 5.5, the Internet Mail Service does not require the authentication used between Exchange servers within an Exchange organization before it allows the use of an extended verb to transfer certain information among Exchange servers in the Exchange organization.

In Exchange 2000 Server, the SMTP service does not require the authentication used between Exchange servers within an Exchange organization before it allows the use of an extended verb to transfer certain information among Exchange servers in the Exchange organization. Additionally, the SMTP service does not correctly allocate a buffer for this information.

What would this vulnerability enable an attacker to do?

The vulnerability could allow an unauthenticated attacker to exhaust large amounts of memory on the server. This could cause a state where the server would stop responding to requests. In Exchange 2000 Server, the attacker could also, in the worst case, be able to cause remote code execution.

How could an attacker exploit this vulnerability?

An unauthenticated attacker could seek to exploit this vulnerability by connecting to an SMTP port on the Exchange server and by issuing a specially-crafted extended verb request. These requests can allocate memory on the server and can cause a denial of service. In Exchange 2000 Server, it is also possible to craft the request causing the SMTP service to fail in such a way that an attacker could execute code. This could allow an attacker to take any action on the system in the security context of the SMTP service. By default, the SMTP service runs as Local System.

Because Exchange 2000 Server uses the Windows 2000 SMTP service, does the vulnerability affect the SMTP service in Windows 2000?

No. The vulnerability does not affect the Microsoft SMTP service on systems that are running Windows 2000 that do not have Exchange 2000 Server installed.

The vulnerability also does not affect the Microsoft SMTP services that

Securiteam: [NT] Vulnerability in Exchange Server Could Allow Arbitrary Code Execution (MS03-046)

can be installed on Microsoft Windows NT® Server 4.0 or on Microsoft Windows XP.

Does the vulnerability affect the SMTP service in Exchange Server 2003?

No. The SMTP service in Exchange Server 2003 only accepts the SMTP extended verb request from Exchange servers within the same Exchange organization.

Can this be exploited directly by using e-mail?

No. This vulnerability could not be exploited by sending a specially-crafted e-mail message to a mailbox that is hosted on an Exchange server. An attacker would have to connect directly to the SMTP port on an Exchange server.

What does this patch do?

For Exchange Server 5.5 the patch removes the vulnerability by requiring that the authentication used between Exchange servers within an Exchange organization is used before an Exchange server accepts the SMTP extended verb requests.

For Exchange 2000 Server the patch removes the vulnerability by requiring that the authentication used between Exchange servers within an Exchange organization is used before an Exchange server accepts the SMTP extended verb requests. Additionally, this patch implements correct input validation in the affected buffer.

Does this patch introduce any behavioral changes?

Yes. In order to use the Exchange extended verb, the patch requires authenticated SMTP connections between Exchange servers within an Exchange organization.

Exchange servers automatically authenticate to other Exchange servers that are in the same Exchange organization. Therefore, Exchange servers typically do not require configuration changes.

Microsoft thanks the following for working with us to protect customers:

<mailto:joao.gouveia@vodafone.com> Jo?o Gouveia for reporting the issue described in MS03-046.

ADDITIONAL INFORMATION

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS03-046.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS03-046.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.