

[NT] Vulnerability in SMTP Allows Remote Code Execution (MS04-035)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-10/0043.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 10/13/04

To: list@securiteam.com

Date: 13 Oct 2004 16:27:26 +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 SMTP Allows Remote Code Execution (MS04-035)

SUMMARY

A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles Domain Name System (DNS) lookups. An attacker could exploit the vulnerability by causing the server to process a particular DNS response that could potentially allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system. The vulnerability also exists in the Microsoft Exchange Server 2003 Routing Engine component when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4.

DETAILS

Vulnerable Systems:

* Microsoft Windows XP 64-Bit Edition Version 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=b53e890d-7d6a-4bb4-8e28-15d661014288>>

Download the update (KB885881)

* Microsoft Windows Server 2003 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=d7767455-1ca0-49ea-8f71-76da5d451a07>>

Download the update (KB885881)

Securiteam: [NT] Vulnerability in SMTP Allows Remote Code Execution (MS04-035)

* Microsoft Windows Server 2003 64-Bit Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=b53e890d-7d6a-4bb4-8e28-15d661014288>>

Download the update (KB885881)

* Microsoft Exchange Server 2003 and Microsoft Exchange Server 2003 Service Pack 1 when installed on Microsoft Windows Server 2003 (uses the Windows 2003 SMTP component)

* Microsoft Exchange Server 2003 when installed on Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=313BEC77-0845-46D4-BB43-06C792ADB2EA>>

Download the update (KB885882)

Immune Systems:

* Microsoft Windows NT Server 4.0 Service Pack 6a

* Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6

* Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4

* Microsoft Windows XP, Microsoft Windows XP Service Pack 1, and Microsoft Windows XP Service Pack 2

* Microsoft Windows XP 64-Bit Edition Service Pack 1

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

* Microsoft Exchange Server 5.0 Service Pack 2

* Microsoft Exchange Server 5.5 Service Pack 4

* Microsoft Exchange 2000 Server Service Pack 3

* Microsoft Exchange Server 2003 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 3 or Microsoft Windows 2000 Service Pack 4

Affected components:

* Microsoft Windows XP 64-Bit Edition Version 2003 SMTP component

* Microsoft Windows Server 2003 SMTP component

* Microsoft Windows Server 2003 64-Bit Edition SMTP component

* Microsoft Exchange Server 2003 Routing Engine component

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0840>>

CAN-2004-0840

Mitigating Factors for SMTP Vulnerability

* By default, the SMTP component is not installed on Windows Server 2003, Windows Server 2003 64-Bit Edition, or Windows XP 64-Bit Edition Version 2003.

* By default, the SMTP component is not installed when Internet Information Services (IIS) 6.0 is installed.

* Windows NT Server 4.0, Windows 2000, Windows XP, Windows XP 64-Bit Edition, Exchange Server 5.0, Exchange Server 5.5, and Exchange 2000 Server are not affected by this vulnerability.

Workarounds for SMTP Vulnerability

* Use a firewall to block incoming TCP protocol network traffic on port 53 for Windows Server 2003 systems using the SMTP component, regardless of

if Exchange is installed.

Use a firewall to block TCP protocol network traffic on port 53. Do not block UDP traffic on port 53 or the server will be unable to make any DNS queries to resolve domain names.

Impact of Workaround: Port 53 is used for DNS queries and responses. By blocking the TCP protocol on port 53, all DNS name resolution must be done through the UDP protocol. Large DNS responses sent through TCP can be split between multiple packets, while responses sent through UDP must fit within a single UDP packet. This means that if you rely only on UDP for DNS name resolution, you may be unable communicate with domains that return more IP addresses than can fit in a single UDP packet. Typically, each entry in a DNS response requires 16 bytes. Therefore, a single UDP response packet can contain approximately 30 IP addresses.

Note: It is possible to minimize potential disruptions of DNS name resolution by implementing a metabase key. For detailed information about this, see Microsoft Knowledge Base Article <http://support.microsoft.com/?id=820284> 820284. Setting the metabase key will allow SMTP to use partial UDP name resolution responses to route mail. It will not prevent TCP responses from being sent to the server, and setting the metabase key is not a substitute for blocking TCP on port 53. This metabase key affects only SMTP, and it will not affect the name resolution behavior of other services and applications.

* Block TCP protocol network traffic on Windows Server 2000 Service Pack 3 or Service Pack 4 systems with Microsoft Exchange Server 2003 with no service pack installed.

If you have defined External DNS Servers, you can block TCP protocol network traffic on port 53 between the Exchange server and all external DNS servers. Follow these steps to check if External DNS Servers have been configured on your Exchange server. Start the Exchange System Manager and for each server:

- * Expand the Protocols container.
- * Expand the SMTP container.
- * For each SMTP virtual server:
 - * Open the SMTP virtual server Properties.
 - * Select the Delivery tab.
 - * Click the Advanced button.
 - * Click the Configure button.

Block TCP traffic on port 53 between any external DNS servers listed and the Exchange server. If there are no external DNS servers listed, you do not have to take any action. However, Microsoft strongly recommends that you apply the security update or service pack for Exchange 2003 so that you will be protected if the configuration of your server changes in the future.

Impact of Workaround: This workaround will affect only SMTP traffic on the Exchange system. It will not affect name resolution by other applications and services. The external DNS servers configured in Exchange System Manager are used only by the SMTP and Exchange Routing services. With TCP

Securiteam: [NT] Vulnerability in SMTP Allows Remote Code Execution (MS04-035)

traffic from these servers blocked on port 53, Exchange will automatically use partial UDP name resolution responses to route mail. There is no need to set a metabase key as described above for Windows Server 2003 in order for SMTP to take advantage of partial responses. It is possible that some mail will still be unable to be delivered. This will happen only if a valid email server IP address is not found in a partial UDP response.

* Do not block both TCP and UDP for port 53. Doing so will cause all DNS name resolution to fail on the server.

* If your server hosts applications that are configured to use only TCP for DNS responses, then this workaround will cause those applications to be unable to resolve domain names to IP addresses.

* If your server is used primarily as an SMTP-based email server or Exchange server, messages addressed to domains that return large DNS responses may not be processed or delivered.

FAQ for SMTP Vulnerability

What is the scope of the vulnerability ?

A remote code execution vulnerability exists in the Windows Server 2003 SMTP component because of the way that it handles DNS lookups. An attacker who successfully exploited this vulnerability could take complete control of an affected system. The vulnerability also exists in Microsoft Exchange Server 2003 when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4.

What causes the vulnerability ?

An unchecked buffer in the Windows SMTP component and in the Exchange Routing Engine component.

What is SMTP ?

Simple Mail Transfer Protocol (SMTP) is an industry standard for delivering e-mail messages 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 is the Exchange Routing Engine component ?

The Exchange Routing Engine component is part of the Exchange Routing Engine Service. The Exchange Routing Engine Service implements the Routing Engine API and determines how e-mail messages are routed through an Exchange system.

Why are there updates for both Windows Server 2003 and Exchange Server 2003 ?

The reason that this issue is addressed in both products is that name resolution functionality that was previously available only in the Exchange Server 2003 Routing Engine component was added to the Windows Server 2003 SMTP component. This is why you should install the update for Windows Server SMTP component update (KB885881) on Windows Server 2003

Securiteam: [NT] Vulnerability in SMTP Allows Remote Code Execution (MS04-035)

regardless of whether you have Exchange Server 2003 installed.

The update for Microsoft Exchange Server 2003 when installed on Microsoft Windows 2000 Service Pack 3 or on Microsoft Windows 2000 Service Pack 4 (KB885882) addresses the issue that is described in this bulletin in the Exchange Server 2003 Routing Engine component.

On Windows 2000, you should install Exchange Server 2003 Routing Engine component update only if you are running Exchange Server 2003 and you have not yet installed Exchange Server 2003 Service Pack 1.

On Windows Server 2003, Exchange uses the Windows Server 2003 SMTP component and bypasses the Exchange Server 2003 Routing Engine component for certain name resolution functions. On Windows 2000 Server, Exchange uses the functionality its Exchange Routing Engine component because this functionality is not available in the Windows 2000 SMTP component.

Is it possible to install the Exchange Routing Engine component update (KB885882) on Windows Server 2003-based systems ?

Yes. It is possible to install the Exchange Routing Engine component update on Windows Server 2003-based systems if you have Exchange Server 2003 installed, but you have not yet installed Exchange Server 2003 Service Pack 1. However, you may not want to because doing this does not help protect against this vulnerability on Windows Server 2003-based systems. It only helps protect against this vulnerability on Windows 2000-based systems. To help protect against this vulnerability on Windows Server 2003-based systems, you must install the Windows Server 2003 SMTP component update (KB885881).

What might an attacker use the vulnerability to do ?

An attacker who successfully exploited this vulnerability could take complete control of the affected system or could cause the SMTP component, and other services that are hosted by Internet Information Services on the same system, to repeatedly fail.

Who could exploit the vulnerability ?

On Exchange Server 2003, or on systems that use the Windows Server 2003 SMTP component, any anonymous user who could deliver a specially crafted message to the affected system could try to exploit this vulnerability.

How could an attacker exploit the vulnerability ?

An attacker could attempt to exploit the vulnerability by creating a specially crafted DNS response message and sending the message to an affected system, which could then cause the affected system to execute code.

What systems are primarily at risk from the vulnerability ?

Systems using Windows 2000 are only vulnerable to this issue when they use Exchange Server 2003. When Exchange Server 2003 Service Pack 1 is installed, systems using Windows 2000 are no longer at risk from this vulnerability.

Securiteam: [NT] Vulnerability in SMTP Allows Remote Code Execution (MS04-035)

Systems using Windows Server 2003 are at risk from this vulnerability when they use the native SMTP component that is provided as part of the operating system, when they run Exchange Server 2003, or when they run Exchange Server 2003 Service Pack 1.

Is the Windows 2000 SMTP component affected ?

No. The vulnerability does not affect the Windows 2000 SMTP component.

Could the vulnerability be exploited over the Internet ?

Yes. An attacker may be able to exploit this vulnerability over the Internet.

What does the update do ?

The update removes the vulnerability by modifying the way that the SMTP component validates the length of a message before it passes the message to the allocated buffer.

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

No. Microsoft had not received any information indicating that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/MS04-035.msp>>
<http://www.microsoft.com/technet/security/bulletin/MS04-035.msp>

=====

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.