

MajorRev: v2.0 Microsoft Security Bulletin MS04-035 – Vulnerability in SMTP Could Allow Remote Code Execution (885881)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2005-02/0024.html>

From: Russ Cooper (*Russ.Cooper_at_TRUSECURE.CA*)

Date: 02/08/05

Date: Tue, 8 Feb 2005 16:06:59 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS04-035:
Vulnerability in SMTP Could Allow Remote Code Execution (885881)

Bulletin URL:

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

Reason for Revision: Bulletin updated to advise of the availability of an update for Exchange 2000 Server
Version Number: 2.0

Issued Date: Tuesday, October 12, 2004

Revision Date: Tuesday, February 08, 2005

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Patch(es) Replaced: None

Caveats: The security update for Exchange 2000 Server Service Pack 3 requires, as a prerequisite, the Exchange 2000 Server Post-Service Pack 3 (SP3) Update Rollup. You must install the Update Rollup for Exchange 2000 (KB870540) before you install the security update that is provided in this security bulletin. This security update will detect whether the Update Rollup is installed. If the Update Rollup is not installed, you will be directed to the download Web site. For more information, see Microsoft Knowledge Base Article 870540. To download the prerequisite update, visit this Web site.

Tested Software:

Affected Software:

* Microsoft Windows XP 64-Bit Edition Version 2003

<<http://tinyurl.com/6ru5u>>

* Microsoft Windows Server 2003

<<http://tinyurl.com/3w2r2>>

* Microsoft Windows Server 2003 64-Bit Edition 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)

<<http://tinyurl.com/6ru5u>>

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

<<http://tinyurl.com/5oej4>>

* Microsoft Exchange 2000 Server Service Pack 3
<<http://tinyurl.com/5y2w5>>

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
- * Microsoft Exchange 2000 Server Routing Engine component

Technical Description:

* SMTP Vulnerability – CAN-2004-0840: 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 and in Microsoft Exchange 2000 Server Service Pack 3.

Revision History:

- * v1.0 – 10/12/2004: Bulletin published
- * v1.1 – 11/9/2004: Bulletin updated to clarify restart requirement for Windows Server 2003 and Windows XP 64-Bit Edition Version 2003
- * v2.0 – 2/8/2005: Bulletin updated to advise of the availability of an update for Exchange 2000 Server

This email is sent to NTBugtraq automatically as a service to my subscribers. (v4.01.1837.24459)

Cheers,

Russ – Senior Scientist – TruSecure Corporation/NTBugtraq Editor

--

NTBugtraq Editor's Note:

Most viruses these days use spoofed email addresses. As such, using an Anti-Virus product which a

--