

Alert: Microsoft Security Bulletin – MS03–003

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-01/0013.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 01/23/03

Date: Wed, 22 Jan 2003 18:50:55 -0500

From: Russ <Russ.Cooper@RC.ON.CA>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

<http://www.microsoft.com/technet/security/bulletin/MS03-003.asp>

Flaw in how Outlook 2002 handles V1 Exchange Server Security Certificates could lead to Information Disclosure (812262)

Originally posted: January 22, 2003

Summary

Who should read this bulletin: Administrators of Microsoft Outlook 2002 systems using V1 Exchange Server Security certificates for encryption.

Impact of vulnerability: Information Disclosure

Maximum Severity Rating: Moderate

Recommendation: Administrators of Microsoft Outlook 2002 systems using V1 Exchange Server Security certificates for encryption should apply the patch immediately.

Affected Software:

– Microsoft Outlook 2002

End User Bulletin: An end user version of this bulletin is available at:

http://www.microsoft.com/security/security_bulletins/ms03-003.asp.

Technical description:

Microsoft Outlook 2002 provides the facility to encrypt e-mails sent between e-mail recipients. Encryption is used to prevent parties other than the intended recipients from reading the contents of an e-mail. Outlook uses public key certificates to facilitate the exchange of the cryptographic keys that are used in the encryption process, and Outlook offers a number of different options as to what type of certificates can be used. S/MIME certificates are the most commonly used (and are not affected by the vulnerability that is the subject of this bulletin), but there are other certificate options including V1 Exchange Server Security certificates.

A vulnerability exists because there is a flaw in the way Outlook 2002 handles a V1 Exchange Server Security certificate when using it to encrypt e-mail. As a result of this flaw, Outlook fails to encrypt the mail correctly

