

[NT] Flaw in Outlook 2002's Way of Handling V1 Exchange Server Security Certificates Leads To Information Disclosure

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-01/0066.html>

From: support@securiteam.com

Date: 01/23/03

From: support@securiteam.com

To: list@securiteam.com

Date: 23 Jan 2003 17:36:37 +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

Beyond Security would like to welcome Tiscali World Online to our service provider team.

For more info on their service offering IP-Secure, please visit http://www.worldonline.co.za/services/work_ip.asp

Flaw in Outlook 2002's Way of Handling V1 Exchange Server Security Certificates Leads To Information Disclosure

SUMMARY

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 and the message will be sent in plain text. This could cause the information in the e-mail to be exposed when the user believed it to be protected through encryption.

DETAILS

Vulnerable systems:

- * Microsoft Outlook 2002

Mitigating factors:

- * This vulnerability only affects encryption when a V1 Exchange Server Security certificate is used. S/MIME encryption, which is the most widely used form of e-mail encryption used by Outlook, is not affected.
- * This vulnerability only affects Outlook 2002 and only when sending HTML e-mail.

Patch availability:

Download locations for this patch

- * Microsoft Outlook 2002:

<http://microsoft.com/downloads/details.aspx?FamilyId=F20A2E4B-E458-48F0-B0CB-7E73C0BB4884&displayla>
<http://www.microsoft.com/office/ork/xp/journ/olk1006a.htm>
<http://www.microsoft.com/office/ork/xp/journ/olk1006a.htm> (administrative update only)

Note: This and other Office updates can be obtained at

<http://office.microsoft.com/productupdates>
<http://office.microsoft.com/productupdates>.

What's the scope of the vulnerability?

This vulnerability could result in a user, who had Outlook 2002 configured to use a V1 Exchange Server Security certificate for e-mail encryption, sending e-mail that the user believed to be encrypted when it in fact was not.

If an attacker were able to intercept the e-mail, the e-mail could be read as plain text, instead of being protected through encryption.

What is a digital certificate?

Digital certificates are a familiar fixture within public-key cryptography. In public-key cryptography, there are two keys: the private key, which must be kept secret, and the public key, which is intended to be shared with the world. In order for the public key to be shared effectively, there needs to be a way to learn whose it is, how it can be used, and to verify that the information is bona fide. Digital certificates provide a way to do this.

A digital certificate combines a public key with information about it – who owns it, what purposes it can be used for, when it expires, and so forth. When a user needs a digital certificate, he or she gets it from an organization known as a Certificate Authority (CA). The CA not only creates the certificate, it also digitally signs it, thereby vouching for the information in it and preventing it from being modified without detection.

What is a V1 Exchange Server Security Certificate?

A V1 Exchange Server Security certificate is one of the encryption certificate options that is available when Outlook 2002 is used in conjunction with a Microsoft Exchange mail server. In this configuration, the Exchange mail server can act as a CA and issue certificates to the Outlook clients. One type of certificate it can issue is the V1 Exchange Server Security certificate – however the default certificate type in this configuration is an S/MIME certificate.

Is there a flaw in V1 Exchange Server Security certificates?

No – it is important to recognize that the flaw is in the way Outlook handles this type of certificate, and not in the certificates themselves.

You've mentioned S/MIME – what is it?

S/MIME stands for Secure/Multipurpose Internet Mail Extensions. S/MIME provides a consistent way to send and receive MIME encoded data securely. Based on the popular Internet MIME standard, S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption).

For a description of S/MIME and information about digital certificates, see Microsoft Knowledge Base article Q195724, RFC 2633 section 1, and the article Working with the Outlook 2000 Security Model.

Is S/MIME affected by this vulnerability?

No – this vulnerability is restricted to situations where V1 Exchange Server Security certificates are being used for encryption.

How do I tell what type of certificate Outlook is using to send and receive encrypted e-mail?

You can tell what type of certificate Outlook 2002 is using for encryption by checking Tools|Options|Security|Security Settings. If the security settings show that the "secure message format" is "Exchange Server Security", then Outlook 2002 is using a V1 Exchange Server Security certificate.

You've talked about encryption, but certificates can be used for digitally signing e-mail as well. Is this application of certificates affected?

No, digital signing is unaffected – this vulnerability only affects encryption using Exchange Server Security certificates.

What causes the vulnerability?

The vulnerability results because Outlook 2002 does not correctly use V1 Exchange Server Security certificates when such certificates are selected for encryption. The result of the error is that the e-mail message is not encrypted

What's wrong with encryption in Outlook 2002 when the V1 Exchange Server Security Certificate is used?

There is a flaw in the way Outlook processes a request to use the V1

Exchange Server Security certificate to encrypt an e-mail message. As a result of this flaw, the certificate is not used properly and the message is sent in plain text.

What could this vulnerability enable an attacker to do?

It would allow an attacker who had the ability to intercept e-mail messages between two parties to read those e-mails even if the parties believed them to be encrypted.

How could an attacker exploit this vulnerability?

To exploit this vulnerability, an attacker would need to have the ability to intercept e-mail between parties who were using V1 Exchange Server Security certificates for encryption, or have access to the infrastructure where those e-mails were being stored, such as access to mail servers. Given this access, an attacker could read e-mails that users believed to be protected by encryption.

What does the patch do?

The patch eliminates the vulnerability by ensuring that Outlook 2002 uses the V1 Exchange Server Security certificate correctly when it is selected as the certificate to be used for encryption operations.

ADDITIONAL INFORMATION

The information has been provided by

<mailto:0_43316_E51E4D7D-DECD-43AE-9A29-36080E8D4C3C_US@Newsletters.Microsoft.com>
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.