

[NT] E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-12/0016.html>

From: support@securiteam.com

Date: 12/05/02

From: support@securiteam.com

To: list@securiteam.com

Date: 5 Dec 2002 12:52:38 +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

E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

SUMMARY

Microsoft Outlook provides users with the ability to work with e-mail, contacts, tasks, and appointments. Outlook e-mail handling includes receiving, displaying, creating, editing, sending, and organizing e-mail messages. When working with received e-mail messages, Outlook processes information contained in the header of the e-mail which carries information about where the e-mail came from, its destination, and attributes of the message.

A vulnerability exists in Outlook 2002 in its processing of e-mail header information. An attacker who successfully exploited the vulnerability could send an especially malformed e-mail to a user of Outlook 2002 that would cause the Outlook client to fail under certain circumstances. The Outlook 2002 client would continue to fail so long as the especially malformed e-mail message remained on the e-mail server. The e-mail message could be deleted by an e-mail administrator, or by the user via another e-mail client such as Outlook Web Access or Outlook Express, after which point the Outlook 2002 client would again function normally.

DETAILS

Securiteam: [NT] E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

Affected Software:

- * Microsoft Outlook 2002

Mitigating factors:

- * Outlook 2002 clients connecting to e-mail servers using the MAPI protocol are not affected. Only Outlook 2002 clients using POP3, IMAP, or WebDAV protocols are vulnerable.
- * The vulnerability does not affect Outlook 2000 or Outlook Express.
- * The vulnerability is a denial of service vulnerability only. The attacker would not be able to access the user's e-mail or system in any way. The vulnerability could not be used to read, delete, create, or alter the user's e-mail.
- * If an attacker was able to send a specially malformed e-mail that successfully exploited this vulnerability, the specially malformed e-mail could be deleted either by an e-mail administrator, or by the user via another e-mail client such as Outlook Web Access or Outlook Express. Once the especially malformed e-mail has been removed, normal operation would resume.

Patch availability:

Download locations for this patch

- * Microsoft Outlook 2002:

<<http://office.microsoft.com/downloads/2002/olk1005.aspx>>
<http://office.microsoft.com/downloads/2002/olk1005.aspx>

Note: This and other Office updates can be obtained at <http://office.microsoft.com/productupdates>.

What's the scope of the vulnerability?

This is a denial of service vulnerability. An attacker who successfully exploited this vulnerability could cause a user to be unable to use Outlook 2002 to access their e-mail.

The vulnerability could not be used by an attacker to access the user's e-mail or system in any way, nor does it pose any risk to e-mail servers. The only effect of a successful attack would be the failure of Outlook 2002 when the user attempted to access the e-mail server. Removing the especially malformed e-mail message from the e-mail server would return the Outlook client to normal operation.

What causes the vulnerability?

The vulnerability results because of a flaw in the way Outlook 2002 processes e-mail header information. Processing an email with a particular type of malformed header could cause Outlook 2002 to fail.

What is Outlook?

Microsoft Outlook, which ships as part of Microsoft Office, provides users with the ability to work with e-mail, contacts, tasks, and appointments.

Securiteam: [NT] E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

Using Outlook for handling e-mail includes the ability to receive, display, create, edit, send, and organize e-mail messages.

What's an e-mail header?

E-mail servers and clients need information that tells them how to process incoming and outgoing e-mails. This information is provided within the e-mail through header fields. Examples of the type of information contained in e-mail header fields include the sender's and receiver's addresses, the time at which the mail was sent, and the name of the mail server that received the mail.

What's wrong with the way Outlook 2002 handles e-mail headers?

In the vulnerability at issue here, Outlook 2002 doesn't correctly process a certain type of invalid information that could be contained in a header field. If an Outlook 2002 client attempted to access an e-mail message containing the specially malformed information using POP3, IMAP, or WebDAV as the access protocol, the Outlook client would fail.

What are the POP3, IMAP, and WebDAV protocols?

POP3 (defined in RFC 1939), IMAP (defined in RFC 2060), and WebDAV (defined in RFC 2518) are protocols that can be used to access e-mail servers to send and receive mail. If your e-mail server is on an Internet Service Provider's server, you are likely using POP3 or IMAP to access your e-mail. WebDAV is a set of extensions to the HTTP protocol and is used by Outlook clients when accessing Hotmail.

Another protocol, MAPI, is commonly used by enterprise's for their e-mail systems. However, systems using MAPI are not affected by this vulnerability.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could cause a user to be unable to access their e-mail using Outlook 2002. The Outlook 2002 client could continue to fail until corrective action has been taken, usually by the e-mail administrator.

How might an attacker exploit this vulnerability?

An attacker could attempt to exploit this vulnerability by sending a specially malformed e-mail message to a user who uses Outlook 2002 to access an e-mail server via the POP3, IMAP, or WebDAV protocol. Upon connecting to the server and processing the email, the Outlook client would fail. The user would be unable to access e-mail on the e-mail server until the specially malformed e-mail message is removed.

Why might Outlook 2002 continue to fail as long as the specially malformed e-mail remains on the e-mail server?

If the especially malformed e-mail message remains on the e-mail server, the Outlook 2002 client would fail each time it encountered the message.

Is this true even in the case of POP3 mail? In that protocol, the mail resides on the client once it's been read, so why would the mail need to

Securiteam: [NT] E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

be deleted from the server?

When Outlook downloads mail from a POP3 server, it converts it during the download into another format, known as MAPI. The vulnerability lies in the code in Outlook 2002 that effects this conversion. As a result, if an Outlook 2002 client attempted to download an attacker's mail from a POP3 server, the POP3-to-MAPI conversion would fail and the mail would not be removed from the server. As a result, even in the POP3 case, normal processing would require deleting the mail from the server

Who could exploit the vulnerability?

This vulnerability could be exploited by any attacker who could craft and send the specially malformed e-mail message

Would the vulnerability enable the attacker to read e-mail on the server?

No. Even if an attacker were able to successfully exploit this vulnerability, no e-mail messages would be lost or compromised.

What would the user need to do to restore normal operation?

To restore normal operation, the especially malformed e-mail would need to be removed from the e-mail server. There are two ways to do this:

- * The user could use another e-mail client such as Outlook Web Access or Outlook Express to delete the e-mail, or

- * An e-mail administrator could delete the e-mail.

Is Outlook 2000 affected?

The Gold version of Outlook 2000 is affected. However, Service Release 1, Service Pack 2, and Service Pack 3 all eliminate the vulnerability. Microsoft typically releases security patches only for the current service pack and the previous one; we do this because service packs are the best way to keep one's system secure. For instance, in the case of Outlook 2000, the service packs that have been delivered over the 3 years since Outlook 2000 Gold was released eliminate a large number of bugs, including several serious security vulnerabilities. The simplest and most effective way to eliminate all of them — including this vulnerability — is to stay up to date on service packs.

Is Outlook Express affected?

No. Outlook Express is not affected by this vulnerability.

Is Outlook 98 affected?

No. Outlook 98 is not affected by this vulnerability.

What does the patch do?

The patch addresses the vulnerability by correcting the flaw and causing Outlook 2002 to correctly process e-mails that contain the invalid header information described above.

ADDITIONAL INFORMATION

Securiteam: [NT] E-mail Header Processing Flaw Could Cause Outlook 2002 to Fail

The information has been provided by

<mailto:0_41746_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.