

[VulnWatch] Bypassing SMTP Content Protection with a Flick of a Button

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-09/0014.html>

From: Aviram Jenik (aviram@beyondsecurity.com)

Date: 09/12/02

From: "Aviram Jenik" <aviram@beyondsecurity.com>

To: <vulnwatch@vulnwatch.org>

Date: Thu, 12 Sep 2002 15:45:13 +0200

Bypassing SMTP Content Protection with a Flick of a Button

Article reference:

<http://www.securiteam.com/securitynews/5YPOA0K8CM.html>

SUMMARY

Forget underground hacking tools. How about using Outlook Express as your attack platform?

Beyond Security's SecurITeam has discovered a new method of bypassing many SMTP-based content filter engines.

This discovery is alarming since it requires from the attacker nothing more than an Outlook Express client and employs a rarely-used feature called 'message fragmentation and re-assembly' that is available in Outlook Express. Using this feature, an attacker can send e-mails that will bypass most SMTP filtering engines including gateway Virus scanners, content filters, Firewalls that do SMTP checking, etc.

DETAILS

One of the least known features of Outlook Express allows Internet and Intranet users to split up sent messages. This allows slow connecting users to send smaller segments of a larger email in multiple emails, whereas the receiving client will automatically join them into a single message. This RFC documented feature called "Message Fragmentation and Reassembly" (RFC2046, section 5.2.2.1) allows anyone to bypass most of the security restrictions imposed on email messages, due to the fact that messages are spliced into smaller segments that will not be detected by virus scanners or other content testing mechanisms.

Possibly affected:

Any email filtering, virus checking, and content checking mechanism that

VulnWatch: [VulnWatch] Bypassing SMTP Content Protection with a Flick of a Button

is unable to assemble a fragmented email to its complete form.

Technical details:

The main idea behind the RFC 2046 message fragmentation is to enable users to send large files as several partial messages, while making it transparent to the recipient, who will receive a single message rather than multiple smaller files.

Fragmentation and Reassembly example:

If a binary attachment is broken into two pieces, the first piece might look something like this:

```
X-Weird-Header-1: Foo
From: Bill@host.com
To: joe@otherhost.com
Date: Fri, 26 Mar 1993 12:59:38 -0500 (EST)
Subject: First mail (part 1 of 2)
Message-ID:
MIME-Version: 1.0
Content-type: message/partial; id="ABC@host.com";
        number=1; total=2
```

```
X-Weird-Header-1: Bar
X-Weird-Header-2: Hello
Message-ID:
Subject: Audio mail
MIME-Version: 1.0
Content-type: application/binary
Content-transfer-encoding: base64
```

VIRUS

And the second half might look something like this:

```
From: Bill@host.com
To: joe@otherhost.com
Date: Fri, 26 Mar 1993 12:59:38 -0500 (EST)
Subject: Second mail (part 2 of 2)
MIME-Version: 1.0
Message-ID:
Content-type: message/partial;
        id="ABC@host.com"; number=2; total=2
```

SIGNATURE

When the fragmented message is reassembled, the resulting message will look something of the sorts of:

```
X-Weird-Header-1: Foo
From: Bill@host.com
To: joe@otherhost.com
```

VulnWatch: [VulnWatch] Bypassing SMTP Content Protection with a Flick of a Button

Date: Fri, 26 Mar 1993 12:59:38 -0500 (EST)
Subject: Mail
Message-ID:
MIME-Version: 1.0
Content-type: application/binary
Content-transfer-encoding: base64

VIRUS
SIGNATURE

Since the emails traversing through the product will be the first email and the second email, and not the completed form, any product looking for the phrase "VIRUS SIGNATURE" will fail to detect the Virus, and the message will pass undetected. Similarly, if compressed files are involved, a product will try to decompress them in order to look into its content, but will be unable to do so since each email contains only a fragment of the compressed file.

So far, the only client that we found to support this feature with a "flick of a button" is Microsoft's Outlook Express. This mail client supports an option that allows fully transparent fragmentation and reassembly of messages. The reassembly feature is enabled by default, while the fragmentation feature is not. Note though, that it can be easily enabled by going to: Tools -> Accounts -> Choose your email account -> Advanced -> Sending / Break apart messages larger than [...]. No other mail client we have checked supports this feature including Microsoft Outlook. However, Outlook Express is widely used in both Corporate and Home environments making this issue a possible high-risk situation.

Impact:

Anyone wishing to bypass SMTP filtering engines can utilize the mentioned method to bypass most types of content checking, and deliver its payload to the end-client without any trouble, whether it is a Virus, Trojan or a file type that is not allowed by the corporate policy.

Workaround:

It seems that by embedding email footer (company disclaimer, privacy note, etc) to each outgoing email traversing through the content filter it is possible to completely hamper the effective usage of this attack. However, since this is an RFC documented feature that may be used in Outlook Express for legitimate purposes, this legitimate usage will be hampered as well.

A vendor solution to this vulnerability would be to include a reassembling agent at the server that will not allow any non-reassembled message to traverse through it.

Vendor response – Check Point:

"Neither the latest 4.1 nor the latest NG versions of FW-1 are

VulnWatch: [VulnWatch] Bypassing SMTP Content Protection with a Flick of a Button

vulnerable to this problem. A few details follow:

1. FW-1 does not directly analyze the body of attachments. In that respect, the vulnerability is not applicable to FW-1.
2. FW-1 has the capability to easily filter these types of messages, by specifying "message/partial" in the "Strip MIME of type:" section of the resource definition.
3. FW-1 does serve as a platform for third party vendors to check attachments for viruses via the "CVP" OPSEC mechanism. When defining a CVP server, a message box is presented to the administrator (when approving the resource) that says:

"When CVP server is used it is recommended to strip MIME of type 'message/partial'. Do you want to add 'message/partial'?"

Pressing "Yes" will automatically add 'message/partial' to the appropriate place in the resource definition.

We therefore believe is safe to say that not only are we not vulnerable to this problem ourselves, we also protect 3rd party opsec partners from falling for this pitfall."

Vendor response – GFI:

GFI MailSecurity for Exchange/SMTP 7.2 has been updated to detect this exploit as "fragmented message" through its email exploit detection engine and quarantines it at server level.

GFI patch URL:

GFI's latest version of MailSecurity for Exchange is patched against this problem. For more information, see:

<<http://www.gfi.com/mailsecurity/>> <http://www.gfi.com/mailsecurity/>

Vendor response – Symantec:

"Symantec has been aware for some time of the potential malicious use of this email feature. As a result, all currently supported Symantec gateway products, by default, block multi-part MIME messages at the gateway. While this is a configurable feature of Symantec gateway products and can be enabled if multi-part email is required, the rejection of segmented messages should be a part of a company's comprehensive security policy to restrict potentially harmful content from the internal network.

Additionally, should known malicious code be delivered to a client computer in this manner, the Symantec and Norton AntiVirus scanning products will detect it when it is reassembled and downloaded to the client computer and/or during attempted execution on the targeted computer. As always, if previously unknown malicious code is being distributed in this manner, Symantec Security Response will react and send updated virus definitions via LiveUpdate to detect the new threat."

VulnWatch: [VulnWatch] Bypassing SMTP Content Protection with a Flick of a Button

A full formal response from Symantec should be shortly available at:

<<http://securityresponse.symantec.com/avcenter/security/SymantecAdvisories.html>>

<http://securityresponse.symantec.com/avcenter/security/SymantecAdvisories.html>

(Under "Multiple SMTP bypass")

Vendor response – TrendMicro:

"We have confirmed that our product InterScan VirusWall 3.5x for NT is affected by the vulnerability mentioned by Beyond Security Ltd. regarding fragmented e-mails. In order to resolve this problem, we have released a patch in order to address this particular concern for InterScan VirusWall for NT. The said patch can be downloaded from the following FTP server:

<<ftp://ftp-download.trendmicro.com.ph/Gateway/ISNT/3.52/>>

<ftp://ftp-download.trendmicro.com.ph/Gateway/ISNT/3.52/>

The said hotfix is named:

Hotfix_build1494_v352_Smtp_case6593.zip

The hotfix mentioned above contains a Readme file which should include the necessary instructions on how to apply the patch.

Our other mail gateway product, InterScan MSS v5.01 is not affected by this vulnerability provided that you apply the latest hotfixes which can be downloaded from our website at:

<<http://www.antivirus.com/download>> www.antivirus.com/download

"

Vendor response – SonicWALL:

We could not assert whether SonicWALL is vulnerable to this attack and were unable to receive a response from SonicWALL despite several contact attempts.

Vendor response – NAI:

We could not assert whether any of NAI's products is vulnerable to this attack and were unable to receive a response from NAI despite several contact attempts.

Vendor response – Cisco:

The following response was received from Cisco's security contact on September 1st:

"We are still working on this issue, and I do not have the latest information. We will follow up in a few days."

CERT:

We have received a response from CERT indicating that they have informed several vendors about the issue, but were unable to receive an updated status in the last few weeks. CERT is tracking this issue as VU#836088.

ADDITIONAL INFORMATION

GFI Email Security Testing Zone:

GFI has set up an email security testing engine that can be used to test your system for the mentioned vulnerability. This testing zone is available at:

<<http://www.gfi.com/emailsecuritytest/>>
<http://www.gfi.com/emailsecuritytest/>

The information has been provided by <<mailto:noamr@beyondsecurity.com>>
Noam Rathaus, Beyond Security Ltd.

--
Aviram Jenik
Beyond Security Ltd.
<http://www.BeyondSecurity.com>
<http://www.SecuriTeam.com>

Know that you're safe: <http://www.AutomatedScanning.com>

- **Previous message:** [Foundstone Labs: "\[VulnWatch\] Foundstone Labs Advisory – Buffer Overflow in Savant Web Server"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)