

Bypassing SMTP Content Protection with a Flick of a Button

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-09/0123.html>

From: Aviram Jenik (aviram@beyondsecurity.com)

Date: 09/12/02

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

To: <bugtraq@securityfocus.com>

Date: Thu, 12 Sep 2002 15:45:03 +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

SecurityFocus Bugtraq: 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, wh