

Re: Security flaw in how Outlook verifies digital signatures

Source: <http://www.tech-archive.net/Archive/Outlook/microsoft.public.outlook/2005-02/3326.html>

From: Vanguard (use_ReplyTo_at_domain.invalid)

Date: 02/19/05

Date: Sat, 19 Feb 2005 01:38:27 -0600

"Roberto Franceschetti" <roberto_remove_n.o.s.p.a.m_tag@logsat.com>
wrote in message news:1WzRd.56892\$pc5.4933@tornado.tampabay.rr.com...

> Jeff,

>

> *Simple exploit. I use my own Verisign digital certificate to sign an
> email. I then alter the from in the email to make it appear from
> Microsoft. I then send the signed email to my competitor. He sees an
> email coming from Microsoft, digitally signed, with a valid signature,
> but unfortunately he's using Outlook which does not warn him that the
> sender does not match the certificate (if he had only used Mozilla or
> Outlook Express he'd see flags everywhere...). The email will talk
> about a new non-existent vulnerability, and perhaps I will attach an
> infected attachment, with a copy of maybe Optix Pro to get a backdoor
> into his system...*

>

> *Am I stupid because I used my own certificate...? Not really, you see,
> somebody stole my private key which I upladed onto my ISP's public ftp
> server to make it easier for me to access it while traveling... in
> court my lawyer would be having a field day proving my innocence as a
> victim of fraud, and in the meantime I've caused irreparable harm to
> my competitor. All because Outlook is the only email client that did
> not warn him about the sender not being the one who signed the
> email...*

>

> *...this is only one example of abuse of the exploit.*

>

> *Yes, if you look deep down in the signature a *very* computer-savvy
> user will eventually understand that the sender is not really the
> person who signed the email. But I stress on the computer savvy words.
> Your average and even above average computer user will have no idea
> that the email was not from Microsoft, as the vast majosrity of users
> have no idea how these certificates work. They just care about "the
> email is digitally signed" and "my email program says it's valid".*

>

> Roberto Franceschetti

microsoft.public.outlook: Re: Security flaw in how Outlook verifies digital signatures

> roberto at sign logsat.com
>
> "Jeff Stephenson [MSFT]" <stephenson@online.microsoft.com> wrote in
> message news:18zrcqipebceb.dlg@jeff.stephenson.microsoft.com...
>> On Fri, 18 Feb 2005 04:55:06 GMT, Roberto Franceschetti wrote:
>>
>>> Please look in particular at the words "This proves to the recipient
>>> that
>>> the message is from you and not from an imposter"
>>
>> And this is exactly what Outlook does, if you look at the actual
>> *signature* on the message instead of the (incredibly easily forged)
>> "From". As I said before, anybody that can actually sign the message
>> with
>> your certificate isn't going to be stupid enough to send it with
>> their
>> address; to see who the message is from, always check the signature,
>> not
>> the From.
>>
>> If you really care about the legitimacy of snail mail, do you check
>> the
>> return address on the envelope, or compare the actual ink signature
>> to a
>> known copy of the person's signature? Same thing in email – check
>> the
>> signature. [Actually, given current image technology, digital
>> signatures
>> are *much* better than ink signatures...]
>>
>> --
>> Jeff Stephenson
>> Outlook Development
>> This posting is provided "AS IS" with no warranties, and confers no
>> rights
>
>

And why you need to PROTECT your private key at all times. If your key is stolen, invalidate it. Then anyone getting digitally signed documents from "you" will see that your certificate is no longer valid.

Whether your e-mail was signed or not, relying on a comparison against the sender info in the headers, especially those headers that the *sender* inserts in their own composed *data* within the DATA command, is flawed in the first place. Since the sender-composed headers cannot be used to determine the sender accurately, comparing them against the digital signature is stupid. That's like having a con man show his ID who you then verify with his buddy con man: you are using the WRONG source to validate the digital signature.

microsoft.public.outlook: Re: Security flaw in how Outlook verifies digital signatures

In your example, you assume the recipient never ever bothered to actually look at the credentials recorded within your certificate and that they never ever bothered to check your certificate had not been revoked. They got a digitally signed e-mail and only use the spoof-able headers to determine who authored the content of the e-mail? Then why bother going to the trouble to digitally sign in the first place? Just spoof the headers as you were intending to do in the first place. Digital signatures are worthless unless you actually look them up. The identity and e-mail address are encoded in the security certificate.

--

Post your replies to the newsgroup. Share with others.
E-mail reply: Remove "NIXTHIS" and add "#VS811" to Subject.
