

Security Flaw in how Outlook verifies Digital Signatures

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-02/0409.html>

From: Roberto Franceschetti (*roberto_remove_n.o.s.p.a.m_tag_at_logsat.com*)

Date: 02/17/05

Date: Thu, 17 Feb 2005 21:24:30 GMT

This report is also available graphically at
<http://www.logsat.com/Signatures>

On 10/21/2004 the following vulnerability was reported to Microsoft:

Security Flaw with Digital signatures in Microsoft Outlook –
Emails in Microsoft Outlook digitally signed with S/MIME using either a commercial personal certificate like Verisign or using a certificate issued by MS Certificate Server can be altered. Outlook will not show any warnings about the email being changed, the digital signature will still be reported valid even though the message content has been modified and parties involved in the signatures changed.

This is an extremely serious flaw as I can change any digitally signed emails I want without Outlook ever noticing.

After several emails with Microsoft and CERT during the months that followed, no fixes have been issued to correct this security flaw. It is only now that I am making this information public after all my attempts to have Microsoft resolve the problem have failed.

The following are 3 digitally signed messages. The 1st one is a valid, unmodified email from Roberto Franceschetti (roberto at logsat.com) to support at logsat.com: (follow the hyperlinks for the email's source and screenshots)

Screenshot at <http://www.logsat.com/Signatures/Valid.gif>

Email's source at <http://www.logsat.com/Signatures/Valid.msg>

The following one has been "hacked" so that the sender now appears to be "Hackers Franceschetti" (hackers@logsat.com). Note that Outlook states that the email is absolutely valid, and that the certificate is Valid and Trusted. This is most definitely not the case, as I've altered the original message to make it appear as a different person actually sent it. Imagine the scenario where a digital signature is supposed to unequivocally identify a sender, but now this email that appears to be sent by "hackers" appears legitimate, and a poor victim will trust it and send the hacker any confidential information he is asked for... (follow the hyperlinks for the

alt.computer.security: Security Flaw in how Outlook verifies Digital Signatures

email's source):

Screenshot at <http://www.logsat.com/Signatures/Hacked1.gif>

Email's source at <http://www.logsat.com/Signatures/Hacked1.msg>

This 3rd email is yet another variation showing how a digitally signed email can further be forget without Outlook ever raising warning flags (follow the hyperlinks for the email's source):

Screenshot at <http://www.logsat.com/Signatures/Hacked2.gif>

Email's source at <http://www.logsat.com/Signatures/Hacked2.msg>

The full emails with the conversations between myself, Microsoft and CERT can be found here (<http://www.logsat.com/Signatures/emails.asp>). I hope that by making this information public all the users who rely on digital signatures will be aware of this severe security flaw in Microsoft Outlook, and will take other precautions to ensure the identity of users in digitally signed emails they receive.

Roberto Franceschetti

LogSat Software

roberto at sign logsat.com