

Re: MS Exchange Relay Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-10/0012.html>

From: Greg Crowe (*GregCrowe_at_FCCFURN.COM*)

Date: 10/01/03

Date: Wed, 1 Oct 2003 08:24:56 -0700
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Jake,

Tek-tips has an excellent thread covering this topic (with conclusive answers).

<http://www.tek-tips.com/gviewthread.cfm/lev2/3/lev3/15/pid/10/qid/655444>

(URL may wrap)

Quick summary:

Make sure you are logging Exchange SMTP interface events. Now check your event log for event ID 2010 (successful login) for bogus accounts as well as 4183 (failed login).

This is classic behavior for Outlook clients infected with the w32.swen.a@mm (SARC has a nice summary page:

<http://www.sarc.com/avcenter/venc/data/w32.swen.a@mm.html>).

Big thanks for James3838 on the tek-tips forums for helping all of us out on this one!

Regards,

– Greg Crowe

> -----Original Message-----

> *From: Hovermale, Jake [mailto:hovermalej@BEINETWORKS.COM]*

> *Sent: Thursday, September 25, 2003 2:59 PM*

> *To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM*

> *Subject: MS Exchange Relay Authentication*

>

>

> *We've seen quite a few Exchange Servers recently being used*

> *as relays. Relay restrictions are set to "allow all computers*

> *which successfully authenticate to relay, regardless of the*

> *list above." We've removed this option and added the*

> *appropriate servers to the granted computers list and the*

NT-Bugtraq: Re: MS Exchange Relay Authentication

> *problem goes away. Some remote users may need to reset their*
> *email settings to use the local ISP's smtp server but that's*
> *how it should be anyway.*
>
> *We've seen tens of thousands of messages on average piled up*
> *in the queues. Exchange 2000 handles it much better than 5.5.*
> *5.5 seems to crash the server more often than not. 2000*
> *handles it but your Internet browsing may not work too well.*
> *We've done some searching and have found a few others with*
> *similar problems.*
>
> *It seems that account passwords are being cracked. At that*
> *point the spammer can successfully authenticate and voila,*
> *free relay server. Removing the 'authenticate-relay-option'*
> *solves the relay problem but not the fact that the passwords*
> *are so easily cracked. We've been enabling the maximum*
> *setting on the MExchangeTransport SMTP Protocol to look for*
> *eventlog errors to track down the compromised accounts. We've*
> *also suggested resetting all account passwords with stronger*
> *settings, removing all unnecessary accounts, and patching the*
> *systems. All this is the usual stuff but we've seen this on*
> *systems with all but the most up to date patch set so we're*
> *not at all sure where vulnerability is or how the passwords*
> *are being cracked.*
>
> *Anyone have any insight?*
>
> *Thank you,*
>
> *Jake*
>
>
>
>
> -----
> *Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!*
>
> *With a growth rate exceeding 110%, the TICSAs security*
> *practitioner certification is one of the hottest IT*
> *credentials available. And now, for a limited time, you can*
> *save 33% off of the TICSAs certification exam! To learn more*
> *about the TICSAs certification, and to register as a TICSAs*
> *candidate online, just go to*
>
> <http://www.trusecure.com/offer/s0100/>

Wondering as to whether the list is running? The NTBugtraq archives are updated first before messages are emailed to subscribers. Check the archives first to see if you have missed any messages;
<http://www.ntbugtraq.com/archives>

NT-Bugtraq: Re: MS Exchange Relay Authentication
