

MS Exchange Relay Authentication

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-10/0005.html>

From: Hovermale, Jake (*hovermalej_at_BEINETWORKS.COM*)

Date: 09/25/03

Date: Thu, 25 Sep 2003 17:58:49 -0400
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

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 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 TICSA security practitioner certification is one of the hottest IT credentials available. And now, for a limited time, you can save 33% off of the TICSA certification exam! To learn more about the TICSA certification, and to register as a TICSA candidate online, just go to

NT-Bugtraq: MS Exchange Relay Authentication

<http://www.trusecure.com/offer/s0100/>
