

Re: New Microsoft Exchange Server Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-11/0088.html>

From: Thor (*thor_at_hammerofgod.com*)

Date: 11/15/03

To: "Paul Kurczaba" <paul@myipis.com>, "'Tom Burns'" <tburns@torcausa.com>, <focus-ms@securityfocus.com>
Date: Sat, 15 Nov 2003 10:15:23 -0800

Some gems to point out in this "vulnerability."

It requires the guest account be turned on, and that the smtp virtual server is directly accessible for auth. I love this quote from the guy who "discovered" this:

"If the guest account is enabled (on Exchange 5.5 and 2000), even if your login fails, you can send mail, because the guest account is there as a catchall," he said. "Even if you think you've done everything (to secure the server), you are still open to spammers."

Done everything except disable the guest account, he means. I like the way they nicely dance over "The guest account is a way for administrators to let visitors use a mail server anonymously, but because of security issues, the feature is generally not enabled. " I also like how they call "cleaning Code Red" leaving the guest account active (and presumably still part of the admin group). Duh.

But my favorite is: ' "It is really inexcusable for a company that claims security is its top priority," he said.'

No, it is inexcusable for a college kid to charge someone to misconfigure their servers, and leave the guest account on (and let's not go into how they got Code Red in the first place) and go on about it as if it was someone else's fault.

T

----- Original Message -----

From: "Paul Kurczaba" <paul@myipis.com>

To: "'Tom Burns'" <tburns@torcausa.com>; <focus-ms@securityfocus.com>; <security-basics@securityfocus.com>

Sent: Friday, November 14, 2003 7:32 PM

Subject: New Microsoft Exchange Server Vulnerability

Here is a link that I ran across. There is a new flaw that allows spammers to send emails through Microsoft Exchange.

SecurityFocus Microsoft: Re: New Microsoft Exchange Server Vulnerability

http://zdnet.com.com/2100-1105_2-5107904.html?tag=zdfd.newsfeed

-Paul Kurczaba

-----Original Message-----

From: Tom Burns [mailto:tburns@torcausa.com]

Sent: Tuesday, November 11, 2003 9:00 AM

To: focus-ms@securityfocus.com

Subject: Exchange SMTP Hole?

Good morning all,

I have an exchange server that's been running for quite some time (over a year) and had it locked down to prevent relay (spam). It is patched all the way up to 3a.

I checked my queues yesterday an