



White Paper

Microsoft Spam Server

Aaron Greenspan

Date: November 12, 2003
Topic Area: Security

Overview

On July 18, 2002, in a highly publicized “Executive E-Mail,” Bill Gates wrote the following: “Six months ago, I sent a call-to-action to Microsoft’s 50,000 employees, outlining what I believe is the highest priority for the company and for our industry over the next decade: building a Trustworthy Computing environment for customers that is as reliable as the electricity that powers our homes and businesses today.”

Now, almost two years after the alarm, Microsoft’s Trustworthy Computing environment arguably still does not exist. The progress that has been made in the effort to clean up the millions of lines of code that constitute Microsoft’s vast library of software programs has taken place mostly in the form of “Service Packs.” And though the band-aid approach is clearly needed, the unfortunate result for consumers is that installing the Windows XP Professional Edition operating system on a typical system now requires downloading no less than 57MB of updates and patches—nearly impossible for a customer with a dial-up internet connection.

To add to the long list of bugs, Think Computer yesterday discovered a fatal flaw in Microsoft

Exchange Server 5.5, a version of the company’s e-mail server software, which is widely used in institutions small and large to relay e-mail messages. Even when a server running Microsoft Exchange is “secure” according to Microsoft’s own standards, the flaw allows anyone to use the server to send hundreds of thousands of pieces of spam daily.

Microsoft has acknowledged that this is a problem in Microsoft Exchange Server 5.5.

Though it is briefly documented under article number Q251149 in the knowledge base on the Microsoft Support web site, the company admits that product’s design did not take flaws in related software applications into account. At this time, Microsoft does not consider

the flaw serious enough to merit a software patch.

Effects

The effects of this problem are far worse than the annoyance derived from receiving a piece of unsolicited mail, or even several of them. Microsoft Exchange Server can be configured to generate error messages for various types of problems, including when messages do not reach their intended recipients. This is of particular concern

The effects of this problem are far worse than the annoyance derived from receiving a piece of unsolicited mail.



with spam, since the addresses for senders and recipients are often randomly generated. For messages that have invalid “To:” addresses, this means the sender will receive an error message, and the administrator of the Exchange server may also receive one. If the “From:” address is invalid, an additional error message will be sent to the administrator of the Exchange server when the error to the sender, who does not really exist, does not go through. Since Exchange Server 5.5 and Exchange Server 2000 accept null sender addresses as valid by design, spammers can use a “From:” address of “<>” and still count on the server to accept it. Therefore, for spam messages with malformed addresses, there exists the potential for up to four error messages to be generated for every piece of spam, two of which require internet bandwidth to be delivered externally.

When thousands of spam messages and their associated error messages are waiting in an outgoing mail queue, the load on the server is enough to prevent it from completing other mission-critical tasks. In the Windows NT Task Manager, STORE.EXE, the Microsoft Exchange Information Store Service, will often push the CPU utilization to 100% for extended periods of time. As a result, the server may not be able to send or receive valid e-mail, serve web pages, share files and printers, check files for viruses, or run custom business software as it might under normal circumstances.

History of the Problem

The problem with Exchange Server stems from several other glitches in Microsoft products that have plagued users in the past. Most notably, the problems with Microsoft Windows NT Server 4.0 that made the operating system susceptible to attack by the Code Red virus (and its later vari-

ants) are partially to blame for this latest issue.

Versions 4.0 of Microsoft Windows NT Server and Workstation (as well as Windows 2000) ship with a Guest account, designed to allow guests without dedicated user accounts to use a server. Since most organizations do not actually desire this kind of functionality, the Guest account is disabled by default. In addition to the destructive “back door” that the Code Red virus is known for, one of its many other effects is that of enabling the Guest account without the administrator’s knowledge or permission. Though Microsoft’s patch for Code Red closed the back door, it left the status of the Guest account unchanged. Since the Guest account also has no password by default, this allows for a number of potential problems, of which the issue concerning Microsoft Exchange is only one.

Details of the Problem

The vulnerability in Microsoft Exchange Server, which according to Microsoft affects versions 5.5 Service Pack 4 (SP4) and 2000, and may affect other versions as well, allows users to abuse the SMTP capabilities in one of two ways:

- Users can login with the Guest account credentials (which do not require a password) in order to relay e-mail;
- Users are automatically permitted to use the Guest account credentials to relay e-mail if another login fails. In other words, Exchange assumes that the server operator intended to use the Guest account for e-mail relaying, even though this practice is extremely rare and generally not recommended for servers on the internet.

Even in situations where messages are not actually relayed, or messages do not contain



enough data to fill up a broadband internet connection, the error messages that they generate can have just as bad of an effect.

Temporary Solutions

Microsoft recommends disabling Microsoft Exchange notifications for all types of errors if they are clogging the administrator inbox. However, these errors are a good notification of whether or not there is something wrong with your server. Think Computer recommends keeping them on, as long as there is enough disk space to support the volume of messages. (Volume can be extremely heavy—several hundred messages per hour or more—and may depend on the speed of your internet connection.)

To tell if this problem is affecting your server, turn on Maximum logging for SMTP-related items in the Logging tab of the Internet Mail Connector in the Microsoft Exchange Administrator console. After restarting the Internet Mail Service, check the log files in the IMCDATA\LOG directory for excessive activity. Also check the Application Log in the Windows NT Event Viewer.

Unless your server needs the Guest account to be enabled to perform a certain task, it should be disabled immediately. Leaving the Guest account enabled on Windows NT Server 4.0 also potentially allows other problems to occur.

Microsoft also recommends disabling your server's ability to relay messages via SMTP, though for many organizations this is not a practical option.

Recommended Solutions

The best way to remedy the problems caused by the wake of Code Red is to categorically pro-

hibit Microsoft Exchange Server from using the Guest account to relay messages via SMTP. Organizations that are using the Guest account to relay messages internally should set up a dedicated user for this purpose with a secure password. Microsoft has not indicated that it will take any action on the matter, however, so only the Temporary Solutions outlined above will work for the time being.

Related Problems

There are a number of related problems with Microsoft Exchange. According to Microsoft, the product works as designed, but we question whether or not the intended designs of certain features actually make sense in the context of a network where spammers probe IP addresses for vulnerable SMTP servers on a minute-by-minute basis.

As mentioned previously, Exchange Server versions 5.5 and 2000 allow null "From:" addresses (see Appendix A), which are often used by spammers. Though human senders rarely to never use null "From:" addresses, mail servers do use them on a regular basis to deliver Non-Deliverable Reports (NDRs). Disabling a mail server's ability to process messages from "<>" would therefore impinge on the server's functionality, since it would be difficult to tell when a message did not go through. On the flip side, it would give spammers one less way to deliver unsolicited messages. Therefore, though this behavior conforms with the SMTP RFC, it opens a loophole that is frequently exploited.

Microsoft Exchange also allows various combinations of malformed "From:" addresses that are not null. Though Microsoft claims that it is faithful to SMTP RFC which outlines how addresses should be interpreted as valid, this provides a chan-



nel for abuse, as well. It should be noted for the sake of comparison that similar tests on Linux-based servers using sendmail did not reveal the same vulnerabilities, since these servers perform directory lookups for any domain name before delivering a message.

Microsoft claims that if Exchange performed directory lookups for domain names, so that mail could only be delivered to valid users, spammers would have a better idea of who to target. We argue that not performing directory lookups gives spammers an incentive not just to send out more messages, but more messages on a higher order of magnitude, since finding the right username then requires sending messages to thousands of randomized addresses in order to find the ones that actually work.

Though Microsoft is aware of this view, at the current time it will not provide Exchange Server version 5.5 or 2000 customers with the option of directory lookup unless they upgrade to Exchange Server 2003, which supports the option. It maintains that it has made the correct product design choices on behalf of its customers. Judging from the number of users experiencing floods of SMTP traffic related to the aforementioned issues, we are not so sure.

Useful Links

“Guest Account Allows Relaying Regardless of Routing Restrictions”

[http://support.microsoft.com/
default.aspx?scid=kb;en-us;251149](http://support.microsoft.com/default.aspx?scid=kb;en-us;251149)

“XIMS: Microsoft SMTP Servers May Seem to Accept and Relay E-Mail Messages in Third-Party Tests”

[http://support.microsoft.com/
default.aspx?scid=kb;en-us;304897](http://support.microsoft.com/default.aspx?scid=kb;en-us;304897)

“Report a Security Vulnerability”

[https://s.microsoft.com/technet/treeview/
default.asp?url=/technet/security/bulletin/alertus.asp](https://s.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/alertus.asp)

For More Information

For more information about the issues discussed in this White Paper, contact Think Computer via e-mail at info@thinkcomputer.com. Or, visit Think Computer on the World Wide Web at <http://www.thinkcomputer.com>.

Microsoft and Exchange Server 5.5 are registered trademarks of Microsoft Corporation. All other names may be trademarks or registered trademarks of their respective owners.

Copyright © 2003 Think Computer Corporation. All Rights Reserved.

Last Updated November 19, 2003.



Appendix A

Affected Microsoft Exchange 5.5 SP4 Server SMTP Log (35 Second Excerpt)

```
11/11/03 1:59:23 PM : <<< I0: |221 ATT.COM
|
11/11/03 1:59:23 PM : <<< 221 ATT.COM
11/11/03 2:00:01 PM : A CONNECTION TO 216.200.145.19 WAS ESTABLISHED.
11/11/03 2:00:01 PM : <<< I0: |220 IMTA01.MTA.EVERYONE.NET ESMTF POSTFIX
|
11/11/03 2:00:01 PM : <<< 220 IMTA01.MTA.EVERYONE.NET ESMTF POSTFIX
11/11/03 2:00:01 PM : >>> EHLO VULNERABLE.SERVER.COM

11/11/03 2:00:02 PM : <<< I0: |250-IMTA01.MTA.EVERYONE.NET
250-PIPELINING
250-SIZE 20480000
250-ETRN
250 8BITMIME
|
11/11/03 2:00:02 PM : <<< 250-IMTA01.MTA.EVERYONE.NET
250-PIPELINING
250-SIZE 20480000
250-ETRN
250 8BITMIME

11/11/03 2:00:02 PM : >>> MAIL FROM:<> SIZE=2171

11/11/03 2:00:04 PM : <<< I0: |250 0k
|
11/11/03 2:00:04 PM : <<< 250 0k
11/11/03 2:00:04 PM : >>> RCPT TO:<${RANDOMIZE3T@NETSCAPE.COM}>

11/11/03 2:00:05 PM : <<< I0: |550 <${RANDOMIZE3T@NETSCAPE.COM}>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:05 PM : <<< 550 <${RANDOMIZE3T@NETSCAPE.COM}>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:05 PM : >>> RSET

11/11/03 2:00:05 PM : <<< I0: |250 0k
|
11/11/03 2:00:05 PM : >>> MAIL FROM:<> SIZE=2135

11/11/03 2:00:06 PM : <<< I0: |250 0k
|
11/11/03 2:00:06 PM : <<< 250 0k
11/11/03 2:00:06 PM : >>> RCPT TO:<${RANDOMIZE3T@NETSCAPE.COM}>

11/11/03 2:00:06 PM : <<< I0: |550 <${RANDOMIZE3T@NETSCAPE.COM}>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
```



```
11/11/03 2:00:06 PM : <<< 550 <$RANDOMIZE3T@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:07 PM : >>> RSET

11/11/03 2:00:07 PM : <<< I0: |250 0k
|
11/11/03 2:00:07 PM : >>> MAIL FROM:<> SIZE=2188

11/11/03 2:00:07 PM : <<< I0: |250 0k
|
11/11/03 2:00:08 PM : <<< 250 0k
11/11/03 2:00:08 PM : >>> RCPT TO:<$RANDOMIZE6E@NETSCAPE.COM>

11/11/03 2:00:09 PM : <<< I0: |550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:09 PM : <<< 550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:10 PM : >>> RSET

11/11/03 2:00:10 PM : <<< I0: |250 0k
|
11/11/03 2:00:10 PM : >>> MAIL FROM:<> SIZE=2155

11/11/03 2:00:11 PM : <<< I0: |250 0k
|
11/11/03 2:00:11 PM : <<< 250 0k
11/11/03 2:00:11 PM : >>> RCPT TO:<$RANDOMIZE6E@NETSCAPE.COM>

11/11/03 2:00:14 PM : <<< I0: |550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:14 PM : <<< 550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:14 PM : >>> RSET

11/11/03 2:00:16 PM : <<< I0: |250 0k
|
11/11/03 2:00:16 PM : >>> MAIL FROM:<> SIZE=2192

11/11/03 2:00:18 PM : <<< I0: |250 0k
|
11/11/03 2:00:18 PM : <<< 250 0k
11/11/03 2:00:18 PM : >>> RCPT TO:<$RANDOMIZE6E@NETSCAPE.COM>

11/11/03 2:00:19 PM : <<< I0: |550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:19 PM : <<< 550 <$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:19 PM : >>> RSET
```



11/11/03 2:00:20 PM : <<< I0: |250 0k
|
11/11/03 2:00:20 PM : >>> MAIL FROM:<> SIZE=2192

11/11/03 2:00:20 PM : <<< I0: |250 0k
|
11/11/03 2:00:21 PM : <<< 250 0k
11/11/03 2:00:21 PM : >>> RCPT TO:<\$RANDOMIZE3T@NETSCAPE.COM>

11/11/03 2:00:21 PM : <<< I0: |550 <\$RANDOMIZE3T@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:21 PM : <<< 550 <\$RANDOMIZE3T@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:21 PM : >>> RSET

11/11/03 2:00:22 PM : <<< I0: |250 0k
|
11/11/03 2:00:22 PM : >>> MAIL FROM:<> SIZE=2148

11/11/03 2:00:23 PM : <<< I0: |250 0k
|
11/11/03 2:00:23 PM : <<< 250 0k
11/11/03 2:00:23 PM : >>> RCPT TO:<\$RANDOMIZE6E@NETSCAPE.COM>

11/11/03 2:00:24 PM : <<< I0: |550 <\$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:24 PM : <<< 550 <\$RANDOMIZE6E@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:24 PM : >>> RSET

11/11/03 2:00:24 PM : <<< I0: |250 0k
|
11/11/03 2:00:24 PM : >>> MAIL FROM:<> SIZE=2148

11/11/03 2:00:25 PM : <<< I0: |250 0k
|
11/11/03 2:00:25 PM : <<< 250 0k
11/11/03 2:00:25 PM : >>> RCPT TO:<\$RANDOMIZE3T@NETSCAPE.COM>

11/11/03 2:00:26 PM : <<< I0: |550 <\$RANDOMIZE3T@NETSCAPE.COM>: RECIPIENT ADDRESS RE-
JECTED: THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
|
11/11/03 2:00:26 PM : <<< 550 <\$RANDOMIZE3T@NETSCAPE.COM>: RECIPIENT ADDRESS REJECTED:
THIS USER DOES NOT HAVE AN ACCOUNT HERE (MTA:IMTA01)
11/11/03 2:00:26 PM : >>> QUIT

11/11/03 2:00:27 PM : <<< I0: |221 BYE