

Update: MS05-011 EYE: Windows SMB Client Transaction Response Handling Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2005-03/0183.html>

From: Marc Maiffret (mmaiffret_at_eeeye.com)

Date: 03/09/05

Date: Wed, 9 Mar 2005 14:07:21 -0800

To: <BUGTRAQ@SECURITYFOCUS.COM>

Windows NT 4.0 was found to be vulnerable to bugs resolved in the MS05-011 patch. Microsoft will not be releasing a public Windows NT 4.0 patch due to the products end of life. Microsoft has however created a private patch for customers whom have paid for extended Windows NT 4.0 support. For more information on extended Windows NT 4.0 support please visit:

[http://www.microsoft.com/presspass/features/2004/dec04/12-03NTSupport.as](http://www.microsoft.com/presspass/features/2004/dec04/12-03NTSupport.asp)

p

But enough of me being a spokesperson to Microsoft customers for Microsoft... ;-)

If your organization is unlucky enough to still have Windows NT 4.0 systems (most due) and your not able to pay for extended support then you do not have a whole lot of options. One way we found to mitigate these attacks, at least some of them, is to enable SMB Signing. This does not truly mitigate the attack but instead it creates change in the SMB protocol that most attack tools I have seen do not support. Therefore it breaks them from being able to successfully exploit remote systems. In the end though an attacker can obviously add support for SMB signing and your back to being vulnerable. It is however better than nothing. For information on how to turn on SMB signing visit:

<http://support.microsoft.com/default.aspx?scid=kb:en-us:161372> Also you should read and implement the NSA Windows NT 4.0 security guidelines as they can in some cases provide more mitigation from attacks:

http://www.nsa.gov/snac/downloads_winnt.cfm?MenuID=scg10.3.1.1 Obviously any change at this level of the OS should be documented because there is a good chance some legacy apps might break.

eEye customers with Blink (Host IPS) are protected from these attacks on NT 4.0 systems regardless of patch level and without impact to application functionality.

Signed,
Marc Maiffret

Chief Hacking Officer
eEye Digital Security
T.949.349.9062
F.949.349.9538

<http://eEye.com/Blink> – End-Point Vulnerability Prevention

<http://eEye.com/Retina> – Network Security Scanner

<http://eEye.com/Iris> – Network Traffic Analyzer

<http://eEye.com/SecureIIS> – Stop known and unknown IIS vulnerabilities

Important Notice: This email is confidential, may be legally privileged, and is for the intended recipient only. Access, disclosure, copying, distribution, or reliance on any of it by anyone else is prohibited and may be a criminal offense. Please delete if obtained in error and email confirmation to the sender.

| -----Original Message-----

| From: Marc Maiffret [mailto:mmaiffret@eeye.com]

| Sent: Tuesday, February 08, 2005 4:14 PM

| To: BUGTRAQ@SECURITYFOCUS.COM

| Subject: EEYE: Windows SMB Client Transaction Response
| Handling Vulnerability

| Windows SMB Client Transaction Response Handling Vulnerability

| Release Date:

| February 8, 2005

| Date Reported:

| August 2, 2004

| Severity:

| High (Remote Code Execution)

| Vendor:

| Microsoft

| Systems Affected:

| Windows 2000

| Windows XP

| Windows Server 2003

| Overview:

| eEye Digital Security has discovered a vulnerability in
| Windows SMB client's handling of SMB responses. An attacker
| who can cause an affected system to connect to the SMB
| service on a malicious host may exploit this vulnerability in
| order to execute code on the victim's machine.

| Technical Details:

| The driver MRXSMB.SYS is responsible for performing SMB
| client operations and processing the responses returned by an

| SMB server service. A number of important Windows File
| Sharing operations, and all RPC-over-named-pipes, use the SMB
| commands Trans (25h) and Trans2 (32h). A malicious SMB server
| can respond with specially crafted Transaction response data
| that will cause an overflow wherever the data is handled,
| either in MRXSMB.SYS or in client code to which it provides
| data. One example would be if the file name and short file
| name length fields in a Trans2 FIND_FIRST2 response packet
| can be supplied with inappropriately large values in order to
| cause an excessive memcpy to occur when the data is handled.
| In the case of these examples an attacker could leverage
| file:// links, that when clicked by a remote user, would lead
| to code execution.

| Protection:

| Retina – Network Security Scanner – has been updated to
| identify this vulnerability.
| Blink – End-Point Vulnerability Prevention – protects from
| this vulnerability.

| Vendor Status:

| Microsoft has released a patch for this vulnerability. The
| patch is available at:
| <http://www.microsoft.com/technet/security/bulletin/MS05-011.msp>

| Credit:

| Yuji Ukai, Derek Soeder

| Related Links:

| Retina – Network Security Scanner –
| <http://www.eeye.com/html/products/retina/index.html>
| Blink – End-Point Vulnerability Prevention –
| <http://www.eeye.com/html/products/blink/index.html>

| Greetings:

| KiP(he is back), altoids, cretz, hsj, commit(it works
| well...), Ink, Rhone, Rose, Mr. White, Chris, Joy, Spot,
| Alena, Brey, and Cristo.

| Copyright (c) 1998-2005 eEye Digital Security Permission is
| hereby granted for the redistribution of this alert
| electronically. It is not to be edited in any way without
| express consent of eEye. If you wish to reprint the whole or
| any part of this alert in any other medium excluding
| electronic medium, please email alert@eEye.com for permission.

| Disclaimer

| The information within this paper may change without notice.
| Use of this information constitutes acceptance for use in an
| AS IS condition. There are no warranties, implied or express,
| with regard to this information. In no event shall the author

| be liable for any direct or indirect damages whatsoever
| arising out of or in connection with the use or spread of
| this information. Any use of this information is at the
| user's own risk.
|