

[NT] Windows SMB Client Transaction Response Handling Technical Details (MS05-011)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-02/0034.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 02/13/05

To: list@securiteam.com

Date: 13 Feb 2005 11:06:06 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Windows SMB Client Transaction Response Handling Technical Details
(MS05-011)

SUMMARY

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.

DETAILS

Vulnerable Systems:

- * Windows 2000
- * Windows XP
- * Windows Server 2003

For detailed information regarding vulnerable systems refer to the advisory linked in the 'Vendor Status' section below.

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

Securiteam: [NT] Windows SMB Client Transaction Response Handling Technical Details (MS05-011)

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 memcopy 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.

Vendor Status:

Advisory release date: February 8, 2005

Date Reported to vendor: August 2, 2004

Microsoft has released an advisory and patches for this vulnerability. The patch is available at:

<http://www.microsoft.com/technet/security/bulletin/MS05-011.msp>

Vulnerability in Server Message Block Could Allow Remote Code Execution

ADDITIONAL INFORMATION

The information has been provided by <mailto:mmaiffret@eeye.com> Marc Maiffret.

The original article can be found at:

<http://www.eeye.com/html/research/advisories/AD20050208.html>

<http://www.eeye.com/html/research/advisories/AD20050208.html>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.