

[NT] DCE RPC Vulnerabilities New Attack Vectors Analysis

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-12/0040.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 12/14/03

To: list@securiteam.com

Date: 14 Dec 2003 14:05:51 +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>

DCE RPC Vulnerabilities New Attack Vectors Analysis

SUMMARY

Core Security Technologies researchers discovered new attack vectors for recently published vulnerabilities in Microsoft Windows operating systems.

These new attack methods were found while researching exploitation conditions for the Workstation Service vulnerability discovered by eEye Digital Security and disclosed in Microsoft security bulletin MS03-049 of November 11, 2003.

They might also apply to other vulnerabilities such as the DCE RPC DCOM and the Messenger service vulnerabilities addresses by bulletins MS03-001, MS03-026, and MS03-043.

We found that by combining three protocol characteristics common to the vulnerabilities mentioned, an attacker can devise more severe, stealthy and low-noise attack vectors than those originally concieved. This creates the opportunity for malicious software to compromise large numbers of vulnerable systems in a massive scale, much like the Blaster and Slammer worms that caused great damage earlier in 2003.

Securiteam: [NT] DCE RPC Vulnerabilities New Attack Vectors Analysis

Core Security Technologies urges users of Microsoft Windows operating systems to deploy the available patches for these vulnerabilities as they effectively fix the problem. Suggested workarounds should be revisited to ensure that they address all currently known attack vectors properly (including the new ones disclosed in this advisory).

DETAILS

Vulnerable systems:

- * Microsoft RPC services running on Windows 2000 and Windows XP

Solution/Vendor Information/Workaround:

Patches are readily available to fix the vulnerabilities and close all known attack vectors.

See Microsoft Security Bulletins [MS03-001], [MS03-026], [MS03-043], [MS03-049]:

- * <<http://www.microsoft.com/technet/security/bulletin/MS03-001.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS03-001.asp>
- * <<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>
- * <<http://www.microsoft.com/technet/security/bulletin/MS03-043.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS03-043.asp>
- * <<http://www.microsoft.com/technet/security/bulletin/MS03-049.asp>>
<http://www.microsoft.com/technet/security/bulletin/MS03-049.asp>

Technical Description – Exploit/Concept Code:

In recent months, several vulnerabilities in the Microsoft RPC code (see [MS03-001], [MS03-026], [MS03-043], [MS03-049]) have been disclosed.

The RPC vulnerabilities account started back in July when LSD disclosed a severe security hole in the DCOM service. Since then, different workarounds were discussed on several security mailing lists but doubt persisted as to which RPC protocol sequences were potential attack gates. This is, obviously, an important factor in determining which ports should be filtered to prevent remote attacks and how other workarounds should be deployed.

We have researched three protocol characteristics which when used together provide the attacker with new severe, stealthy and low-noise attack vectors.

We were able to successfully exploit some of the latest DCE RPC vulnerabilities through less noted ports and even on broadcast addresses.

The following sections provide more specific details about these attack vectors.

Some RPC services listen on high ports

This is a little-known feature that has been omitted from the published alerts to date. The importance of this issue lies in the fact that the

most common filtering rules used on current firewall configurations will allow incoming traffic on these ports.

For instance, the latest Workstation Service vulnerability can be exploited on a high TCP/UDP port. Usually the TCP port is 1025 and the UDP port is higher, depending on system settings.

Some RPC services listen to broadcast traffic

Further tests showed that those attacks conducted with datagram protocols (like UDP) could be targeted to broadcast addresses and still succeed. Our first tests required performing a two-way handshake with each host that responded to the broadcasted query. This situation seems to confuse the native Windows 2000 RPC implementation, so we suspected that this kind of attack could not be built with the stock implementation.

The idempotent bit

RPC has an interesting feature that allows the client to avoid the two-way handshake customary to datagram protocols. This can be enabled by turning on the idempotent flag in RPCv4 request packets. This not only reduces the traffic needed to perform the attack, but it also makes it possible to spoof the request's source. This handshake involves a 20-byte secret number, apparently not easily guessable, that can be avoided by setting the idempotent flag.

We were able to exploit [MS03-026] using 445/TCP 139/TCP 135/TCP 135/UDP and 80/TCP. [MS03-049] can be successfully exploited through 445/TCP 139/TCP and dynamically assigned TCP/UDP ports over 1024. We have not seen public exploits or worms using those ports, and we are not sure whether the Windows API can be bent for this purpose. We used our own DCE RPC implementation that is part of the publicly available Impacket project. Presumably, [MS03-043] (Messenger service) can be exploited using the same techniques, but we have not attempted an attack, although third party reports describe messenger service attacks using UDP broadcasts in the wild.

Firewall bypassing

Since the attack can be conducted over the UDP protocol and that it can be spoofed, it is easy to bypass common filtering rules. Some personal firewalls enable the blocking of traffic on an application basis, but some of the vulnerable services actually run inside the same application that does the DNS resolution. This can be used to the attacker's advantage to reach the vulnerable targets by spoofing the attack packets as if they came from a legitimate server sending DNS responses back to DNS clients on vulnerable workstations.

It is common to see filtering rules like the following:

```
allow UDP packets from DNSSERVER port 53 to WORKSTATION port above 1024
```

The outlined attack vector will pass through the above rule and succeed.

Even personal firewall rules that specify an application will allow these attacks to pass:

```
allow UDP packets from DNSSERVER port 53 to WORKSTATION application
```

services.exe

Conclusions

Patches for the vulnerabilities mentioned have already been made available by Microsoft. Installing them will effectively fix the bugs and close all attack vectors discovered herein.

Workarounds should be revisited to ensure they properly cover these attack vectors.

As a general conclusion, we recommend careful inspection of Windows Service vulnerabilities in order to identify potential avenues of attack related to these services providing RPC endpoints that listen to UDP and TCP traffic on high ports.

Appendix

DCE RPC protocol sequences

A protocol sequence is a "character string that represents a valid combination of an RPC protocol (such as ncacn), a transport protocol (such as TCP), and a network protocol (such as IP)" (see [MSDN]).

What protocol sequences are available?

A standard Windows installation has default services accessible through many protocol sequences. For example, the Workstation Service can be accessed by means of the following:

```
ncacn_ip_tcp:[####]
ncacn_np:[\\PIPE\wkssvc]
ncadg_ip_udp:[####]
```

Notes: #### is a port number above 1024. Datagram based sequences (like ncadg_ip_udp) are also accessible through the broadcast address.

Named pipes (strings like ncacn_np) can be contacted in several ways, via TCP ports 139, 445, 593, and 80.

How easy is it to build an attack over an alternative transport?

Starting from a working attack to an RPC service it is trivial to adapt it to work over other protocol sequences. Of course the attacker must have a DCE RPC implementation that allows her to use her choice of transport, here is where Impacket fits perfectly into the task as changing transports requires no additional effort.

===IMPACKET EXAMPLE=====

```
class ExploitPacket(ImpactPacket.Header):
    OP_NUM = 0x1B # Interface's method number
    def get_header_size(self):
        return 0
    def __init__(self, aBuffer = None):
        ImpactPacket.Header.__init__(self, 0)

class Attack:
    def do(self,host):
```

Securiteam: [NT] DCE RPC Vulnerabilities New Attack Vectors Analysis

```
# The next two lines could be changed to use different protocol
sequences.
#port = 445
#stringbinding = "ncacn_np:%s[\\pipe\\wkssvc]" % host # SMB over
IP/TCP on port 445
port = 135
stringbinding = "ncacn_ip_tcp:%s[%d]" % (host,port) # IP/TCP
transport on the specified port
exploitStub = ImpactPacket.Data()
exploitStub.set_bytes_from_string(exploitpacket)
exploitPacket = ExploitPacket()
exploitPacket.contains(exploitStub)
rpcTransport = transport.DCERpcTransportFactory(stringbinding)
rpcTransport.set_dport(port)
# Uncomment for UDP protocols:
#rpcConn = impacket.dcerpc.dcerpc_v4.DCERPC_v4(rpcTransport)
rpcConn = impacket.dcerpc.dcerpc.DCERPC_v5(rpcTransport)
rpcConn.connect()
rpcConn.bind(SERVICE_UUID) # 20-byte UUID (including version)
rpcConn.send(exploitPacket)
#( ... exploit specific code ...)
rpcConn.disconnect()
```

=====

Retrieving the list of RPC endpoints

Core Security Technologies provides, as part of its free, open source Impacket package (downloadable from <http://oss.coresecurity.com/>), a tool that allows remote enumeration of RPC of services listening and their assigned port numbers and supported transports.

This code is platform independent Python. A similar tool (RPCDUMP) is available from Microsoft.

ADDITIONAL INFORMATION

The advisory can be found at:

<http://www.coresecurity.com/common/showdoc.php?idx=393&idxseccion=10>
<http://www.coresecurity.com/common/showdoc.php?idx=393&idxseccion=10>.

The information has been provided by <mailto:advisories@coresecurity.com>
Core Security Technologies.

=====

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

Securiteam: [NT] DCE RPC Vulnerabilities New Attack Vectors Analysis

=====
=====

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.