CSE 523S: Systems Security

Co

Systems

Spring 2018

Jon Shidal

Plan for Today

- Announcement
  - No class Wednesday
- Security ne
- Understanding vulnera
- Assignment

Why are computers & networks vulnerable?

- Computers
  - Because we write our own software
    - Did we mistakenly or intentionally add vulnerabilities
  - Because we choose software
    - Can we know if it has vulnerabilities?
  - Because software requires input
    - Can inputs be used to trigger a vulnerability?

- Networks
  - IP has an any-to-any communications model
    - Within IP you cannot control who nds you a packet
    - ks have weak
      cation
    - n a packet arrives, you trust ource address
  - Binding between layers and names & addresses are based on trust
    - Insecure services map between network layers (eg, IP to Ethernet), and names to addresses
  - Secure the “channel” only
    - You really want to secure the data and its source, not an address

What have we done so far?

- Computers
  - Explored binaries
  - Explored processes
- Network
  - Explored packets
  - Explored key protocols
  - Explored encryption

What have oth

Lets Look at Vulnerabilities

- Discovery
- Disclosure
- Company Reaction
- CERT (Computer Emergency Response Teams)
- Tools: Metasploit

Lets go in the WABAC machine…

https://en.wikipedia.org/wiki/Mister_Peabody

… to 2003.

July 16, 2003, on bugtraq

Hello,

We have discovered a critical security vulnerability in all recent versions of
Microsoft operating systems. The vulnerability affects default installations
of Windows NT 4.0, Windows 2000, Windows XP as well as Windows 2003 Se

This is a buffer overflow vulnerabi
any Windows operating system, the RPC interface implementing Distributed Component
Object Model services (DCOM). In a result of implementation error i
responsible for instantiation of DCOM objects, remote attackers can
unauthorized access to vulnerable systems.

The existence of the vulnerability has been confirmed by Microsoft
The appropriate security bulletin as well as fixes for all affected platforms
are available for download from http://www.microsoft.com/security/ (MS03-026).

It should be emphasized that this vulnerability poses an enormous threat and
appropriate patches provided by Microsoft should be immediately applied.

We have decided not to publish codes or any technical details with regard to
this vulnerability at the moment.

With best regards,

Members of
The Last Stage of Delirium
Research Group

http://lsd-pl.net

July 16, 2003, on bugtraq

Hello,

We have discovered a critical security vulnerability in all recent versions of
Microsoft operating systems. The vulnerability affects default installations
of Windows NT 4.0, Windows 2000, Windows XP as well as Windows 2003 Server.

This is a buffer overflow vulnerability that exists in
an integral component of
any Windows operating system, the XAO interface
implementing Di
t of Object Model se
implementation
responsible for instantiation jects, remote
attackers can obtain
unauthorized access to vulnerable systems.

The existence of the vulnerability has been confirmed by Microsoft Corporation.
The appropriate security bulletin as well as fixes for all affected platforms
are available for download from http://www.microsoft.com/security/ (MS03-026).

It should be emphasized that this vulnerability poses an enormous threat and
appropriate patches provided by Microsoft should be immediately applied.

We have decided not to publish codes or any technical details with regard to
this vulnerability at the moment.

With best regards,
Members of
The Last Stage of Delirium
Research Group

http://lsd-pl.net

July 16, 2003, on bugtraq

Hello,

We have discovered a critical security vulnerability in all recent versions of Microsoft operating systems. The vulnerability affects default installations of Windows NT 4.0, Windows 2000, Windows XP as well as Windows 2003 Server.

This is a buffer overflow vulnerability that exists in an integral component of any Windows operating system, the RPC interface implementing Distributed Component Object Model services (DCOM). In a result of implementation error in a function responsible for instantiation of DCOM objects, remote attackers can obtain unauthorized access to vulnerable systems.

The existence of the vulnerability has been confirmed by Microsoft Corporation.

The appropriate
l as fix
all affected pl
are available for download fr
http://www.microsoft.com/secu -026).

It should be emphasized that this vulnerability poses an enormous threat and
appropriate patches provided by Microsoft should be immediately applied.

We have decided not to publish codes or any technical details with regard to
this vulnerability at the moment.

What does it do?

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals wit
f incorrect handling of malformed messages. This
particular vulnerability affects a Distributed Component
enabled ports. This interface handles DCOM object
would be able to run code with Local System
ty activation requests that are sent by client machines to

privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the ic RPC ports.

Mitigating factors:

- To exploit this vulnerability, the attacker would require the ability to send a specially crafted request to port 135, 139, 445 or 593 or any other specifically configured RPC port on the remote machine. For intranet environments, these ports would normally be accessible, but for Internet connected machines, these would normally be blocked by a firewall. In the case where these ports are not blocked, or in an intranet configuration, the attacker would not require any additional privileges.
- Best practices recommend blocking all TCP/IP ports that are not actually being used, and most firewalls including the Windows Internet Connection Firewall (ICF) block those ports by default. For this reason, most machines attached to the Internet should have RPC over TCP or UDP blocked. RPC over UDP or TCP is not intended to be used in hostile environments such as the Internet. More robust protocols such as RPC over HTTP are provided for hostile environments.
- To learn more about securing RPC for client and server please refer to http://msdn2.microsoft.com/en-us/library/Aa379441.

What does it do?

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles D
fully exploited this
vulnerability would be able to run code w tem privileges on an affected system. The attacker would be a ny action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on specific RPC ports.

Mitigating factors:

- To exploit this vulnerability, the attacker would require the ability to send a specially crafted request to port 135, 139, 445 or 593 or any other specifically configured RPC port on the remote machine. For intranet environments, these ports would normally be accessible, but for Internet connected machines, these would normally be blocked by a firewall. In the case where these ports are not blocked, or in an intranet configuration, the attacker would not require any additional privileges.
- Best practices recommend blocking all TCP/IP ports that are not actually being used, and most firewalls including the Windows Internet Connection Firewall (ICF) block those ports by default. For this reason, most machines attached to the Internet should have RPC over TCP or UDP blocked. RPC over UDP or TCP is not intended to be used in hostile environments such as the Internet. More robust protocols such as RPC over HTTP are provided for hostile environments.
- To learn more about securing RPC for client and server please refer to http://msdn2.microsoft.com/en-us/library/Aa379441.

What does it do?

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on specific RPC ports.

Mitigating factors:

- To exploit this vulnerability, an attacker would
  RPC port on the remote machine. For intranet environments, these ports would normally be accessible, but for Internet connected machines, these would normally be blocked by a firewall. In the case where these ports are not blocked, or in an intr
  ker would not require any additional privileges.
- Best practices recommend blocking all TCP/IP ports that are not actually being used
  g the Windows Internet Connection Firewall (ICF)
  block those ports by default. For this reason, most machines attached to the Interne
  or UDP blocked. RPC over UDP or TCP is not
  intended to be used in hostile environments such as the Internet. More robust proto
  are provided for hostile environments.
- To learn more about securing RPC for client and server please refer to http://msdn2.microsoft.com/en-us/library/Aa379441.

What does it do?

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this vulnerability would be able to run code with Local System privileges on an affected system. The attacker would be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on specific RPC ports.

Mitigating factors:

- To exploit this vulnera
  e ability to send the specially crafted reque
  any other applicable
  configured RPC port on the remote machi t environments, these ports would normally be accessible, but fo nected machines, these would normally be blocked by a firewall. I re these ports are not blocked, or in an intranet configuration, the attacker would not require any additional privileges.

- Best practices recommend blocking all TCP/IP ports that are not actually being used, and most firewalls including the Windows Internet Connection Firewall (ICF) block those ports by default. For this reason, most machines attached to the Internet should have RPC over TCP or UDP blocked. RPC over UDP or TCP is not intended to be used in hostile environments such as the Internet. More robust protocols such as RPC over HTTP are provided for hostile environments.

What does it do?

Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. The protocol itself is derived from the Open Software Foundation (OSF) RPC protocol, but with the addition of some Microsoft specific extensions.

There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. This particular vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on RPC enabled ports. This interface handles DCOM object activation requests that are sent by client machines to the server. An attacker who successfully exploited this

vulnerability would be able to run co ed system. The attacker would be

able to take any action on the syste ging or deleting data, or creating

new accounts with full privileges.

To exploit this vulnerability, an attacker would need to send a request to the remote computer on

Where is this from?

environments, these ports would normally be accessible, but for Internet connected machines, these would normally be blocked by a firewall. In the case where these ports are not blocked, or in an intranet configuration, the attacker would not require any additional privileges.

- Best practices recommend blocking all TCP/IP ports that are not actually being used, and most firewalls including the Windows Internet Connection Firewall (ICF) block those ports by default. For this reason, most machines attached to the Internet should have RPC over TCP or UDP blocked. RPC over UDP or TCP is not intended to be used in hostile environments such as the Internet. More robust protocols such as RPC over HTTP are provided for hostile environments.

How does MSFT feel about this?

Also known as …

- MS03-026
  - Microsoft security bulletin
- CVE-2003-03
  - Common Vul
- OSVDB-2100
  - Open-Source Vulnerability DB
- BID-8205
  - Bugtraq ID

Has it been exploited?

http://www.cert.org/

Blaster Worm - 2003

- 10s of thousands of machines infected
- Only stopped by patching systems and ISP filtering

Should exploits be publicized?

- Open question

- What should we consider?
  - How hard is it to exploit?
  - Is a fix ready?
  - How should users be
  - Will companies react appropriately?
  - ...

- Thoughts?

Tools: Met

Thank you, HD Moore

First release of Metasploit: 10/2003

Metasploit

https://www.safaribooksonline.com/library/view/metasploit/9781593272883/pr04s03.html

A Brief History of Metasploit

Metasploit was originally developed and conceived by HD Moore while he was employed as a network security engineer. HD realized that he was spending most of his time writing and sanitizing public exploit code, he began to create a flexible and maintainable framework for the creation and development of exploits. He released his first edition of the Perl-based Metasploit in October 2003 with a total of 11 exploits.

Metasploit

https://www.secforce.com/media/presentations/What_you_didnt_know_about_Metasploit.pdf

This first release includes exploits for:

- IIS 5.0 nsiislog.dll POST Overflow

- IIS 5.0 NTDLL via WebDAV (working almost 100% all SPs)

- IIS 5.0 Printer Overflow (o

- **MS03-026 RPC D** (arbitrary pay ul)

- Apache Win32 Chunked Encoding (NT 4.0 a

- Samba trans2open Overflow (Linux and FreeBSD)

- Solaris sadmind Command Execution

- War-FTPD 1.65 PASS Overflow (Win2k)

How do you find it?

But this is just one of hundreds!

Organizing vulnerabilities

- Vendors
  - Microsoft
- Government
  - US-CERT, Mitre
- Community
  - OSVDB, Metasploit

Bounties

Assignment

- For Monday
  - HTAOE: Ch. 3 133-166
- For Wedne
  - HTAOE: Ch 3 167-194