

CSE 523S: Systems Security

Assignment Project Exam Help

Co <https://eduassistpro.github.io/>
Systems Add WeChat edu_assist_pro

Spring 2018
Jon Shidal

Plan for Today

- Announcement
 - No class Wednesday
- Security ne
 - <https://eduassistpro.github.io/>
- Understanding vulnera
 - Add WeChat edu_assist_pro
- 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 sends you a packet
 - We have weak authentication
 - When a packet arrives, you trust source 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

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro
What have oth

Lets Look at Vulnerabilities

- Discovery

- Disclosure

Assignment Project Exam Help

<https://eduassistpro.github.io/>

- Company Reaction

Add WeChat edu_assist_pro

- CERT (Computer Emergency Response Teams)

- Tools: Metasploit

Lets go in the WABAC machine...

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

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

... 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 vulnerability in 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>

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

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 Object Model service implementation responsible for instantiation of objects, 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>

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

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.

1 as follows appropriate

all affected pl

are available for download fr

<http://www.microsoft.com/secure/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.

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

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.

Assignment Project Exam Help

of the existing handling capabilities of the operating system. This is dealt with by the Remote Procedure Call (RPC) protocol. The protocol is designed to be able to handle requests that are sent to a remote system. The protocol is designed to be able to handle requests that are sent to a remote system. The protocol is designed to be able to handle requests that are sent to a remote system.

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

To exploit this vulnerability, an attacker would need to send a specially formed request to the remote system. The request would need to be sent to the remote system. The request would need to be sent to the remote system. The request would need to be sent to the remote system.

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 to the s <https://eduassistpro.github.io/>

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:

5, 139, 445, 593, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839, 840, 841, 842, 843, 844, 845, 846, 847, 848, 849, 850, 851, 852, 853, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873, 874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 888, 889, 890, 891, 892, 893, 894, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 933, 934, 935, 936, 937, 938, 939, 940, 941, 942, 943, 944, 945, 946, 947, 948, 949, 950, 951, 952, 953, 954, 955, 956, 957, 958, 959, 960, 961, 962, 963, 964, 965, 966, 967, 968, 969, 970, 971, 972, 973, 974, 975, 976, 977, 978, 979, 980, 981, 982, 983, 984, 985, 986, 987, 988, 989, 990, 991, 992, 993, 994, 995, 996, 997, 998, 999, 1000

- Best practices recommend blocking all TCP/IP ports that are not actually being used block those ports by default. For this reason, most machines attached to the Internet are intended to be used in hostile environments such as the Internet. More robust protocols 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:

• The ability to exploit this vulnerability requires a specially crafted request

configured RPC port on the remote machine. In hostile environments, these ports would normally be inaccessible, but for intranet machines, these would normally be blocked by a firewall. If 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.

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat: edu_assist_pro

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 could be able to be connected to the system, giving the attacker the ability to perform actions such as deleting any data on the system 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.



Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

How does MSFT feel about this?

~~Assignment Project Exam Help~~

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Also known as ...

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

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Has it been exploited?

<http://www.cert.org/>



Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro



Blaster Worm - 2003

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

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Should exploits be publicized?

- Open question
- What should we consider?
 - How hard is it to exploit?
 - Will be affected?
 - How should users be
 - Will companies react appropriately?
 - ...
- Thoughts?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment Project Exam Help

Tools: Met

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Thank you, HD Moore

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

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

he was spending most of his time v 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)

1) 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)

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

How do you find it?

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro



But this is just one of hundreds!

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro



Organizing vulnerabilities

- Vendors

- Microsoft

Assignment Project Exam Help

- Government-

<https://eduassistpro.github.io/>

- US-CERT, Mitre

Add WeChat edu_assist_pro

- Community

- OSVDB, Metasploit

What else

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Bounties

Assignment Project Exam Help

<https://eduassistpro.github.io/>

Add WeChat edu_assist_pro

Assignment

- For Monday

- HTAOE: Ch. 3 133-166

Assignment Project Exam Help

- For Wedne

<https://eduassistpro.github.io/>

- HTAOE: Ch 3 167-194

Add WeChat edu_assist_pro