

Sri Lanka Institute of Information Technology

**Individual Assignment**

System Networking and Programming

**CVE-2019-0708**

Remote Desktop Services Remote Code Execution Vulnerability

Blue Keep DOS

IT19010236

Balendrarajah Kajanthan

# Table of Content

1. Abstract
2. Introduction

* Who Found CVE 2019-0708.
* How It was Found.
* When It was Found.
* What’s The damage It Cause.
* What are The Exploitation Techniques

1. Exploitation Methods
2. Exploiting
3. Conclusion

**ABSTRACT**

This is about Blue Keep vulnerability exploit which perform a denial os service attack on the target machine. The National Security Agency alerts users that recent Windows 7 vulnerabilities can be "wormable" so that they can be abused and protected by malware. A vulnerability, CVE-2019-0708, that can affect Windows 7 was released by Microsoft in the middle of May.

It didn't seem to happen much for some months. However, an attack was recently seen in the wild which tried to install cryptomining

software on non-patched RDP servers and exposed the Internet to port 3389.

In later versions such as windows 8, windows 10, this vulnerability is fixed. And the development of security patches. For more up-to-date version. This article includes all the facts and information about the weakness and assault as well as the use of a python package Codes which available in github and Exploit DB.

**INTRODUCTION**

## I’m Balendrarajah Kajanthan doing cyber security specialization at SLIIT. For SNP module we need to exploit vulnerable Operating System. So I took windows 7 to exploit. I run windows 7 on VM ware as virtual machine. I took CVE-2019-0708 Remote Desktop Services Remote Code Execution Vulnerability called as Blue Keep Dos. A weakness in remote-execution coding occurs when an unauthenticated intruder logs to a target device using RDP and sends explicitly created requests in Remote Desktop Services formerly known as Terminal Services. It is a pre-authentication weakness and does not require user interaction. An attacker who successfully exploited this vulnerability could use the target program to execute arbitrary code. An intruder can then install programs; view, modify or remove data; or build new user permission accounts.

## An intruder could send a specially designed request to the Remote Desktop Service target systems using RDP to exploit this vulnerability. Blue Keep (CVE-2019-0708) is a security vulnerability that affecting Microsoft Windows' older versions. This vulnerability includes all 32 or 64-bit and all versions of Service Pack that exist in the following Microsoft Windows Operating Systems (OSs), such as

## Windows 2000

## Windows Vista

## Windows XP

## Windows 7

## Windows Server 2003

## Windows Server 2003 R2

## Windows Server 2008

## Windows Server 2008 R2

## Within the Microsoft Windows OSs mentioned above, Blue Keep exists in a remote desktop protocol (RDP). This weakness can be taken advantage of by an attacker to remotely execute code on an insecure device.

## History Of Blue Keep.

## The UK National Cyber Security Center first noticed. Blue Keep security weakness and Microsoft confirmed it on 14 May 2019. The technology expert from the machine Kevin Beaumont on Twitter called a Blue Keep vulnerability.

## Microsoft notes that an attacker can send packets to one of the systems that are specially designed and have RDP enabled. The intruder will be able to perform a variety of activities after packages are submitted successfully: inserting accounts with full user rights, accessing, modifying, or removing information or downloading programs.

## This task, without any contact between the user, must take place before authentication succeeds.Blue Keep is called "wormable" due to the fact that malware will spread to other compromised systems using this vulnerability on a system, and a Blue Keep exploit will be able to spread rapidly in a way close to 2017's WannaCry attacks. Cybersecurity and Infrastructure Security Agency worked with external stakeholders and found that Windows 2000 is Blue Keep vulnerable.

**what makes the Blue Keep vulnerability so critical?**

1. It affects RDP services used by millions of machines worldwide.

2. It allows remote code execution.

3.It can be weaponized to be worm able.

## What is a Vulnerability

A vulnerability is a weakness that a threat actor, such as an attacker, may exploit in order to carry out unauthorized activities within a computer system. To exploit a vulnerability, an attacker must have at least one device or technique that can attach to a weakness in the program. Vulnerabilities in this frame are also known as the surface of attack.

**What is an Exploit?**

Exploitation is the next move after discovering a loophole in an attacker's playbook. Exploits are the means by which hackers can manipulate a vulnerability for malicious activity; these include pieces of software, command sequences, or even open-source exploit kits.

## Exploitation Method

## Here I Install VM Ware on kali Linux. And I install Windows 7 64 Bit on it. And I remotely exploit codes which I found on exploit DB. There I found Blue Keep Exploit python Codes. Using That Codes we can remotely do a DOS attack on windows Operating system which I mentioned above. But Here I choose Windows 7x64 bit OS. Here I used You Tube videos and other websites to perform a demo presentation to exploit using Kali 2020. I got some codes from GitHub But its contain lot of errors then I found codes on Exploit DB.

## Steps To Do Demo Blue Keep

## 01 – Start to run Windows 7 on VMware. Log in it and you have to right click >on my computer and go to properties and set as shown in this picture.

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

02 – we need to find both ip address of kali linux and windows 7. In kali using ifconfig command. In windows we need to open cmd then we need to type ipconfig

A screenshot of a computer screen

Description automatically generated

A screen shot of a computer

Description automatically generated

03 – we need to use ping command in kali terminal and check the connection is fine or not with help of packets send and received fully without lost.

A screen shot of a computer

Description automatically generated

04 – we need to use nmap in kali to check ports are available or not. The port 3389 is used for Blue keep attack.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

05 -After we confirm ports are available, we need to check the vulnerable are available for our ip address of windows with the help of nessus tool. If you don’t have you need to install it with the help of youtube.A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

06- sacn your ip address as shown in this picture and see All kind of vulnerable under critical normal categories.A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

07- After we found Blue Keep vulnerable to our windows 7 ip address we need to download Exploit codes in Exploit DB or in GitHub and download it and ready to exploit. A screenshot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generated

09 – finally By typing python3(name of file).py (ip address of windows) (64 bit or 32 bit)

Pyhton3 46904.py 172.16.189.131 64

You can see Blue Colour codes are running and your windows 7 start to shutting down

## Conclusion

If it is still being running older versions of OSs, need to be protect from the Blue Keep malware.If u Haven't patched your system to help guard against this malware, It's time to do something

about it.

## CISA urges users and administers to review and incorporate effective mitigation steps as soon as possible, the Microsoft Security Warning and Microsoft Client Guidance for CVE-2019-0708.

1. Patch as soon as possible with the latest Microsoft update. In order to fix this vulnerability, Microsoft released security updates. Microsoft has also released updates on a range of OSs, including Windows Vista, Windows XP and Windows Server 2003, which are no longer officially supported. As ever, before installation, Cybersecurity and Infrastructure Security Agency invites users and administrators to test patches.

2. We can upgrade end-of-life OSs. Consider upgrading to a newer, supported OS like Window 10 any EOL OS that is no longer supported by Microsoft.

3. Disable services not used by OS. Disable services This best practice decreases vulnerability exposure.

4. Enable authentication of the network level in Windows 7 and Windows Server 2008, and Windows Server 2008 R2. It allows a client access to be authenticated and essentially mitigates Blue Keep as it needs an unauthenticated user to exploit the vulnerability.

5.Can be blocked Ports 3389 on enterprise perimeter firewall of the Network Transmission Control Protocol (TCP). Since port 3389 is used for starting an RDP session, it prevents an attacker from running Blue Keep outside the user network, blocking it. This will therefore block valid RDP sessions and can not prevent the initiation of unauthenticated sessions in the network.

6.Monitor incoming RDP connections.