BlueKeep CVE-2019-0708

Hannah Mahalia Manalac Susanty (33329151)

Siti Hajar Binte Abdul Malek (33249812)

Lee Jihu (34061648)

Murdoch University

BlueKeep CVE-2019-0708

## Summary of Vulnerability

CVE-2019-0708 also known as BlueKeep is a vulnerability to execute arbitrary code remotely without having to go through normal authentication steps using Windows Remote Desktop Services (RDS). The RDS allows a user to access a remote computer or virtual desktop over the network. BlueKeep was discovered in Microsoft’s Remote Desktop Protocol (RDP) (Chavez, 2019) and affects several operating systems, such as Windows Vista, Windows 7 and Windows XP. This vulnerability has a CVSS score of 9.8 indicating that it is a critical vulnerability that severely affects the confidentiality, integrity and availability of data (National Vulnerability Database, (National Institute of Standards and Technology (NIST), 2019).

The exploitation of this vulnerability requires the attacker to penetrate the target host system using Remote Desktop Protocol and remotely send codes that are specially crafted. After successfully injecting the codes into the kernel, the attacker would have control of the target system and could then have access to create accounts with full rights, install malicious software and read, edit or delete data (Singapore Computer Emergency Response Team, 2019). The biggest characteristic of the BlueKeep vulnerability is that it could be used in the exploitation of other vulnerabilities or amplify existing malware, such as WannaCry by allowing these malwares to self-propagate without any human interaction, similar to a worm (Heller, 2019).

## Proposed Demonstration of Exploit

A 64-bit Windows 7 operating system is required for the demonstration of exploitation. The Remote Desktop Protocol service must be enabled in the target device as it is known to be vulnerable to CVE-2019-0708. A payload will be sent to the target which will cause blue screen of death (BSOD) errors.

References

Chavez, A. (2019, July 9). *Silent Sector: Blog*. Retrieved June 2021, from Silent Sector LLC Web site: https://www.silentsector.com/blog/an-overview-of-bluekeep-cve-2019-0708

National Institute of Standards and Technology (NIST). (2019, May 16). *CVE-2019-0708 Detail*. Retrieved June 2021, from National Vulnerability Database: https://nvd.nist.gov/vuln/detail/cve-2019-0708

Singapore Computer Emergency Response Team. (2019, May 15). *[SingCERT] Microsoft Remote Desktop Services Remote Code Execution Vulnerability (CVE-2019-0708)*. Retrieved June 2021, from Cyber Security Agency of Singapore Website: https://www.csa.gov.sg/singcert/alerts/microsoft-remote-desktop-services-remote-code-execution-vulnerability-cve-2019-0708

Heller, M. (2019, June). *Information Security Threats: BlueKeep (CVE-2019-0708).* Retrieved Junne 2021, from Tech Target Website: https://searchsecurity.techtarget.com/definition/BlueKeep-CVE-2019-0708