**“OS and Application Level Vulnerabilities”**

***Table of Contents***

*Introduction……………………………………………..(1) CVE-2019-0708.…………………………………………(1-3)*

*Summary.…………………………………………(1)*

*Exploit Technique.………………………………...(2)*

*Migitations.………………………………………..(3)*

*CVE-2019-1010200.……………………………………….(4)*

*Summary.……………………………………………(4)*

*Vulnerability Analysis.………………………………(4)*

*Attack Technique.……………………………………(4)*

*Citations.……………………………………………………..(5)*

Daniel Rao

Feb 22nd, 2021

Vince Skinner

**OS and Application Level vulnerabilities**

**Introduction**

A software vulnerability is a glitch, flaw, or weakness present in the software or in an OS (Operating System). The severity of software vulnerabilities advances at an exponential rate. Of course, all systems include vulnerabilities. The thing is whether or not they're exploited to cause damage.

Vulnerabilities proved to be one of the main security trends of 2021. Despite all of the testing, warnings and advice around vulnerability management, it seems the challenges that organizations face in finding and patching vulnerabilities are not going away anytime soon.

Industry research shows that the number of unpatched vulnerabilities continues to increase, stating that patching is typically delayed by 12 days due to staffing issues, while 72% of security professionals surveyed by ServiceNow reported difficulty in prioritizing what needs to be patched.

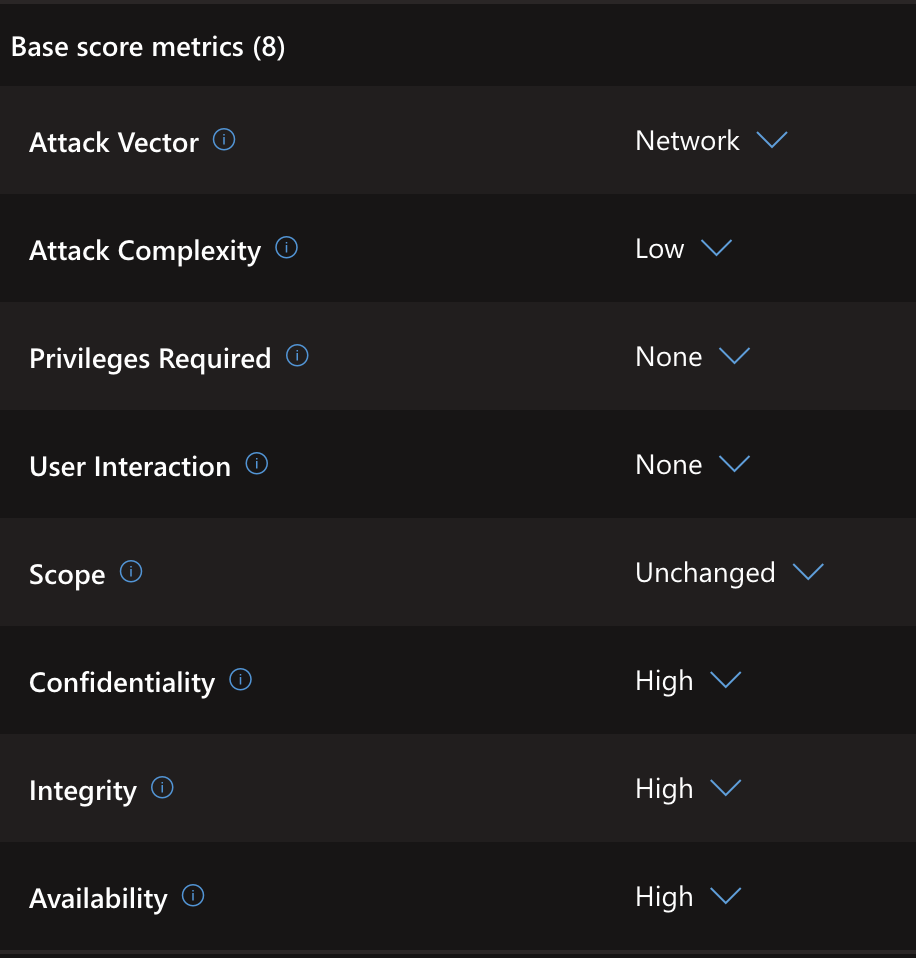
Some of the famous vulnerabilities are as follows:

**CVE-2019-0708 || Remote Desktop Services Remote Code Execution Vulnerability: May 14, 2019**

***Summary:***

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. This vulnerability is pre-authentication and requires no user interaction. An attacker who successfully exploited this vulnerability could execute arbitrary code on the target system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

***Exploit Technique:***

To exploit this vulnerability, an attacker would need to send a specially crafted request to the target systems Remote Desktop Service via RDP. The update addresses the vulnerability by correcting how Remote Desktop Services handles connection requests.***Vulnerability score according to CVE(Common Vulnerabilities and Score):***

***Migitations***

In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as possible even if we plan to leave Remote Desktop Services disabled:

**Disable Remote Desktop Services if they are not required.**

**CVE-2019-1010200 || Google Voice Builder**

***Summary:***

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'). The impact is: Remote code execution with the same privileges as the servers. The component is: Two web servers in the projects expose three vulnerable endpoints that can be accessed remotely.

***Vulnerability Analysis:***

CVSS gets a score of 10 on this type of vulnerability. In this type of vulnerability all confidentiality, integrity and availability are greatly affected as the information here is completely disclosed in all system files being revealed. Not much skill is required in order to conduct this attack and thus access complexity is really low. Authentication is not required to perform this attack.

**Attack Technique:**

The attack vector is: Attacker sends a GET request to the vulnerable endpoint with a specially formatted query parameter. The main culprit of the vulnerability was the improper sanitization of the string that was being input.

The version was fixed after a git commit.

***Citations:***

[*https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708*](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2019-0708)

[*https://www.infosecurity-magazine.com/magazine-features/top-worst-vulnerabilities/*](https://www.infosecurity-magazine.com/magazine-features/top-worst-vulnerabilities/)

[*https://github.com/google/voice-builder/commit/c145d4604df67e6fc625992412eef0bf9a85e26b*](https://github.com/google/voice-builder/commit/c145d4604df67e6fc625992412eef0bf9a85e26b)