Security Advisory-No: 38

19, Feb 2019

Threat Classification: Security Vulnerability

Name: Remote Code Execution Vulnerability (CVE-2019-0547)

Source: Affect following products of Microsoft:

1) Windows 10
2) Windows Server 1803

Distribution: The vulnerabilities can be exploited in the following versions of Microsoft:

- Windows 10 Version 1803 for 32-bit Systems
- Windows 10 Version 1803 for ARM64-based Systems
- Windows 10 Version 1803 for x64-based Systems
- Windows Server, version 1803 (Server Core Installation)

Exploited Vulnerabilities: Hackers can exploit memory corruption vulnerability exists in the Windows DHCP client by sending specially crafted DHCP responses to a client, on successfully exploited the vulnerability, the attacker could run arbitrary code on the client machine for malicious actions.

Recommendations:

1) Use the following official patches to fix the aforementioned vulnerabilities:
    - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0547
2) Whenever possible, run software with minimal access rights and privileges.
3) Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
4) Only use licensed software and avoids download/use of crack and pirated software.
5) In case of any incident, please report to this office.