#REF:106
#Released on:15/04/2020

Microsoft issues patches for 4 zero day bugs

Threat Level
High

Overview
Microsoft has released patches for four zero day vulnerabilities including other 113 security vulnerabilities.

Description
First Vulnerability (CVE-2020-1020)
Vulnerability resides in the Adobe Font Manager library used by the Windows where an attacker could perform remote code execution on the windows system.

Second Vulnerability (CVE-2020-0938)
This Remote code execution vulnerability also resides in the Adobe Type Manager Library that triggers when parsing a malicious OpenType Font.

Third Vulnerability (CVE-2020-1027)
This vulnerability resides in the Windows Kernel, which can be used by attackers to elevate user privileges on a Windows System.

Fourth Vulnerability (CVE-2020-0968)
This is a memory corruption bug resides in the Internet Explorer version 9 and 11 where attackers could remotely compromise Windows based system just by sending malicious link to the victims to open these vulnerable Internet Explorer browsers.

Impact
- Loss of control in your Windows system
- Virus infections possible of ransomware attacks
- Stealing personal information such as usernames and passwords
- Attacker could use your computer as he/she desire

Solution/ Workarounds
- Apply the latest security patch released by the Microsoft.
  Note: For installing the latest Windows security updates, you can head on to Settings → Update & Security → Windows Update → Check for updates on your PC, or you can install the updates manually.

Reference
- https://thehackernews.com/2020/04/windows-patch-update.html

Disclaimer