PTA Cert

Security Advisory-No: 011

12, June 2018

Threat Classification: Vulnerability

Name:

- Graphics Component Vulnerabilities
  (CVE-2018-1010, CVE-2018-1012,CVE-2018-1013, CVE-2018-1015,CVE-2018-1016)

Source: Affect following products of Microsoft:

1) Windows 7
2) Windows 8
3) Windows 10
4) Windows Server 2008
5) Windows Server 2012
6) Windows Server 2016

Distribution: The vulnerabilities can be exploited in following product versions:

1) Windows 7 for (32, 64-bit Systems) SP 1
2) Windows 8.1 for (32, 64-bit Systems)
3) Windows RT 8.1
4) Windows 10 for (32, 64-bit Systems)
5) Windows 10 Version 1511 for (32, 64-bit Systems)
6) Windows 10 Version 1607 for (32, 64-bit Systems)
7) Windows 10 Version 1703 for (32, 64-bit Systems)
8) Windows 10 Version 1709 for (32, 64-bit Systems)
9) Windows Server 2008 for (32, 64-bit Systems) SP 2
10) Windows Server 2008 for (32, 64-bit Systems) SP 2 (Server Core installation)
11) Windows Server 2008 R2 for x64-based Systems SP 1
12) Windows Server 2008 R2 for x64-based Systems SP 1 (Server Core installation)
13) Windows Server 2012
14) Windows Server 2012 (Server Core installation)
15) Windows Server 2012 R2
16) Windows Server 2012 R2 (Server Core installation)
17) Windows Server 2016
18) Windows Server 2016 (Server Core installation)
19) Windows Server, Version 1709 (Server Core Installation)

Exploited Vulnerabilities: Hackers can exploit above vulnerabilities by sending phishing email or instant message to the user that contain a specially crafted file attachment or a suspicious phishing website link. On successful execution of that malicious file attachment or suspicious website, the attacker could gain complete control of an affected system and install, view, delete data and or create accounts with full user rights.

Recommendations:

1) Use following official patches to fix aforementioned vulnerabilities:
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1010
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1012
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1013
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1015
    - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1016

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) Designate a PoC for your network users for seeking assistance and reporting security issues.