PTA Cert

Security Advisory-No: 013

11, July 2018

Threat Classification: Vulnerability

Name: Microsoft Edge Information Disclosure Vulnerability

- ***(CVE-2018-8289, CVE-2018-8325, CVE-2018-8297, CVE-2018-8234)***

Source: Affect following products of Microsoft:

- Microsoft Edge for Windows 10
- Microsoft Edge for Windows Server 2016

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

- Microsoft Edge Windows 10 for 32-bit Systems
- Microsoft Edge Windows 10 for x64-based Systems
- Microsoft Edge Windows Server 2016
- Microsoft Edge Windows 10 Version 1607 for 32-bit Systems
- Microsoft Edge Windows 10 Version 1607 for x64-based Systems
- Microsoft Edge Windows 10 Version 1703 for 32-bit Systems
- Microsoft Edge Windows 10 Version 1703 for x64-based Systems
- Microsoft Edge Windows 10 Version 1709 for 32-bit Systems
- Microsoft Edge Windows 10 Version 1709 for 64-based Systems
- Microsoft Edge Windows 10 Version 1803 for 32-bit Systems
- Microsoft Edge Windows 10 Version 1803 for x64-based Systems

Exploited Vulnerabilities: Hackers can exploit above vulnerabilities by applying social engineering tricks to convincing users to visit suspicious phishing website that contains specially crafted web contents to exploit vulnerabilities. On successful execution of that web contents and suspicious website, the attacker could obtain sensitive information for further malicious activities on the affected system.

Recommendations:

1) Use following official patches to fix aforementioned vulnerabilities:
    - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8297
    - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8289
    - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8325
    - https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-8234
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 avoid download/use of crack and pirated software
5) Designate a PoC for your network users for seeking assistance and reporting security issues