CERT-EU Security Advisory 2017-009

Actively Exploited Critical Zero-Day Vulnerability in Microsoft Office

April 12, 2017 — v1.1

History:

- *11/04/2017 — v1.0: Initial publication*
- *12/04/2017 — v1.1: Adding update information from Microsoft*

Summary

On 8th of April 2017, FireEye researchers detected malicious Microsoft Office Rich Text Format (RTF) document exploiting a zero-day vulnerability to execute a Visual Basic script when an user opens the document [1, 2]. The malicious script gets executed without the need to enable macros, or any other user interaction.

On 10th of April 2017, Proofpoint researchers observed the vulnerability being exploited to distribute the Dridex banking Trojan in a large e-mail campaign [3].

On 11th of April 2017, Microsoft issued a security update to patch the vulnerability (CVE-2017-0199) [5].

Technical Details

The malicious documents embed an OLE2 link object. When the user opens the malicious document, a `.hta` file is downloaded from the Internet. The Microsoft HTA application loads and executes the malicious script. The `.hta` content is disguised as a normal RTF file to evade security products.

The vulnerability is due to the way Microsoft Office products handle HTA files.

Products Affected

All Microsoft Office versions and WordPad on Windows systems are affected by the vulnerability.

Recommendations

Apply security update issued by Microsoft [5].

In the meanwhile, it is recommended to activate Office Protected View to stop the code execution. However, if the user wants to print or edit the malicious document (by clicking on the **Enable Editing** button), the code will be executed.

Another workaround is to set the following registry keys to block RTF files [4]:

- `Software\Microsoft\Office\15.0\Word\Security\FileBlock\RtfFiles` to 2
- `Software\Microsoft\Office\15.0\Word\Security\FileBlock\OpenInProtectedView` to 0

References

[1] FireEye Blog https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html

[2] McAfee Blog https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/

[3] ProofPoint Blog https://www.proofpoint.com/us/threat-insight/post/dridex-campaigns-millions-recipients-unpatched-microsoft-zero-day

[4] Twitter post by Ryan Hanson https://twitter.com/ryHanson/status/851159178416496640

[5] Microsoft security advisory https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199