Zero-day vulnerability in Microsoft Office

Improper input validation

CVE-2017-0199

2017-04-07 2017-04-11

The detected samples are organized as Word files containing Dridex botnet ID 7500 (more specially, RTF files with ".doc" extension name). The exploit works on all Microsoft Office versions, including the latest Office 2016 running on Windows 10. The earliest attack dates to late January, according to McAfee.
According to FireEye, the malware leveraging this vulnerability was used to target Russian-speaking victims. As early as Jan. 25, 2017, lure documents referencing a Russian Ministry of Defense decree and a manual allegedly published in the "Donetsk People's Republic" exploited CVE-2017-0199 to deliver FINSPY payloads.

This vulnerability was also used by Patya.A ransomware in malware outbreak on 27 June, 2017 as one of the attack vectors.

Known malware:

Malware.Binary.Rtf
Dridex botnet
FINSPY
LATENTBOT
Petya.A

Vulnerability details

Advisory: SB2017040901 - Remote code execution in Microsoft Office

Vulnerable component: Microsoft Office

CVE-ID: CVE-2017-0199

CVSSv3 score: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:H/RL:O/RC:C

CWE-ID: CWE-20 - Improper Input Validation

Description:

The vulnerability allows a remote attacker to execute arbitrary code on the target system.

The vulnerability exists due to improper input validation. A remote unauthenticated attacker can create a specially crafted Office document, trick the victim into opening it with Microsoft Office or WordPad and execute arbitrary code on the target system with privileges of the current user.

Successful exploitation of this vulnerability may result in compromise vulnerable system.

Note: the vulnerability is being actively exploited.

Known APT campaigns:

APT against Central Tibetan Administration (CTA)

The attack was launched against the Tibetan government-in-exile named Central Tibetan Administration (CTA). A malware campaign used a malicious Microsoft PowerPoint document shared in the CTA mailing list.

The email contained an attachment "Tibet-was-never-a-part-of-China.ppsx", that installed PE32 ExileRAT.

The attack was revealed on February 4, 2019 by the Cisco TALOS researchers.

CopyKittens targeting Northern Cyprus

In April 2017 CopyKittens has been spreading malicious emails containing a zero-day vulnerability CVE-2017-0199 through a compromised account that belonged to one of the Ministry of Northern Cyprus employee.

BlackTech group

BlackTech group is a cyber espionage group mainly targeting companies in East Asia, particularly Taiwan, and occasionally, Japan and Hong Kong.

The threat group is linked to PLEAD in 2012, Shrouded Crossbow in 2010, and Waterbear cyber operations. To perform attacks BlackTech used a novel right-to-left override (RTLO) technique.

Public Exploits:

- Microsoft Word - .RTF Remote Code Execution [Exploit-DB]
- Microsoft Office Word - Malicious Hta Execution (Metasploit) [Exploit-DB]
- Microsoft Excel - OLE Arbitrary Code Execution [Exploit-DB]

External links:

https://securingtomorrow.mcafee.com/mcafee-labs/critical-office-zero-day-attacks-detected-wild/
https://www.fireeye.com/blog/threat-research/2017/04/acknowledgement_ofa.html
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html
https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

About zero-day vulnerabilities

Zero-day vulnerability is an undisclosed vulnerability in software that hackers can exploit to compromise computer programs, gain unauthorized access to sensitive data, penetrate networks, etc. We consider vulnerability a zero-day when there is no solution provided from software vendor and the vulnerability is being actively exploited by malicious actors.

Zero-day candidate is a potential zero-day vulnerability in software which might have been used in targeted attacks, however there is no evidence to support this suggestion.