MOVING TARGET DEFENSE BLOG

CYBERSECURITY TRENDS, EXPLORING MOVING TARGET DEFENSE
AND PUTTING ENDPOINT THREAT PREVENTION FIRST

CVE-2018-8174 BLOWS THE VBSCRIPT ATTACK DOOR WIDE OPEN

Posted by **MICHAEL GORELIK** on May 25, 2018

Find me on:

In April, researchers at Qihoo 360 Core Security Division discovered a VBScript vulnerability actively exploited in targeted attacks. Since then, it has appeared in additional attack campaigns. The vulnerability, CVE-2018-8174, dubbed "Double Kill", is significant on several counts.

INCREASE IN UAF EXPLOITS

For one, it is a great example of a use-after-free (UAF) memory vulnerability category, a class of vulnerabilities we are seeing with increasing frequency. The heavily exploited Flash vulnerability CVE-2018-4878, reported in early February, also triggered a UAF vulnerability. And the Acrobat Reader double-free vulnerability, CVE-2018-4990 currently exploited in the wild, falls in this category as well. UAF vulnerabilities are particularly dangerous as they can enable the execution of arbitrary code, or, in some cases full remote code execution due to easier access to read and write primitives (read and write to the full process virtual memory).

NEW ATTACK VECTOR

It also opens the door to an entirely new attack vector by expanding the destructive impact of Visual Basic vulnerabilities. Until now, Visual Basic vulnerabilities could only be utilized inside the Internet Explorer browser as only IE supports Visual Basic. This limited their scope and effectiveness. The latest attack that utilized CVE-2018-8174 also used URL Moniker technique to load the VisualBasic exploit directly into the Office process. This significantly changes the current attack vector landscape by introducing previously known Internet explorer browser exploits directly into Office documents This means it can be ported both to spear-phishing campaigns and drive-by campaigns to reach a much wider audience of targets.

We expect to see malspam campaigns exploiting CVE-2018-8174 in the very near future.

TARGETED ATTACK TO MASS MARKET IN DAYS

This vulnerability has set new records in terms of migration from targeted 0-day attack to criminal mass market exploit kit. Attacks in the wild were first discovered at the end of April. Microsoft released a patch on May 8. It was integrated into the Metasploit framework less than two weeks later and within two days was incorporated into the RIG exploit kit. With the addition of this new vulnerability, RIG is likely to see a resurgence in popularity.

HOW TO PROTECT YOURSELF FROM DOUBLE KILL

If you can, patch. Microsoft included a patch for CVE-2018-8174 in it's May 2018 updates.

If you are a Morphisec customer, you are protected even if you cannot patch immediately. Morphisec stops Double Kill across its attack chain. It prevents the exploit execution both from a weaponized Word file and any exploit kit that may deliver the exploit directly into the Internet Explorer browser.

RESOURCES

https://malware.dontneedcoffee.com/2018/05/CVE-2018-8174.html

https://github.com/smgorelik/Windows-RCE-exploits/tree/master/Web/VBScript

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/a82328f9-1f26-e811-a968-000d3a33a34d

http://blogs.360.cn/blog/cve-2018-8174-en/

SEARCH OUR SITE

Keyword...

RECENT POSTS

Parallax: The New RAT on the Block

Remote Employees Offer Different Security Challenges

Why Client-Grade Technology Doesn't Cut It for Cloud Workload Protection

Trickbot Delivery Method Gets a New Upgrade Focusing on Windows 10

Introducing the Morphisec Unified Threat Prevention Platform -- Version 4

Endpoint Security Is Harder than Ever

Trickbot Trojan Leveraging a New Windows 10 UAC Bypass

Morphisec Protects Customers Against Internet Explorer Scripting

Endpoint Detection and Response Is Not the Next Step

Are Guests Safe From a Hotel Data Breach?

POSTS BY TAG

Cyber Security (94)

Endpoint Security (74)

Attack Analysis (45)

Cyber Attacks (45)

Company News (38)

See all