RESEARCH

A new exploit for zero-day vulnerability CVE-2018-8589

By Boris Larin, Anton Ivanov, Vladislav Stolyarov on November 14, 2018. 7:00 am

Yesterday, Microsoft published its security bulletin, which patches a vulnerability discovered by our technologies. We reported it to Microsoft on October 17, 2018. The company confirmed the vulnerability and assigned it CVE-2018-8589.

Acknowledgements

Igor Soumenkov (2igosha) of Kaspersky Lab
Boris Larin (Oct0xor) of Kaspersky Lab

In October 2018, our Automatic Exploit Prevention (AEP) systems detected an attempt to exploit a vulnerability in Microsoft's Windows operating system. Further analysis revealed a zero-day vulnerability in win32k.sys. The exploit was executed by the first stage of a malware installer in order to gain the necessary privileges for persistence on the victim's system. So far, we have detected a very limited number of attacks using this vulnerability. The victims are located in the Middle East.

Kaspersky Lab products detected this exploit proactively using the following technologies:

- Behavioral Detection Engine and Automatic Exploit Prevention for endpoints
- Advanced Sandboxing and Anti-Malware Engine for Kaspersky Anti Targeted Attack Platform (KATA)

Kaspersky Lab verdicts for the artifacts in this campaign are:

- HEUR:Exploit.Win32.Generic
- HEUR:Trojan.Win32.Generic
- PDM:Exploit.Win32.Generic

More information about the attack is available to customers of Kaspersky Intelligence Reports. Contact: intelreports@kaspersky.com

Technical details

CVE-2018-8589 is a race condition present in win32k!xxxMoveWindow due to improper locking of messages sent synchronously between threads.

The exploit uses the vulnerability by creating two threads with a class and associated window and moves the window of the opposite thread inside the callback of a WM_NCCALCSIZE message in a window procedure that is common to both threads.

WM_NCCALCSIZE message in win32k!xxxCalcValidRects

Termination of the opposite thread on the maximum level of recursion inside the WM_NCCALCSIZE callback will cause asynchronous copyin of the lParam structure controlled by the attacker.

```
9e303888 918f64ce win32k!SfnINOUTNCCALCSIZE+0x263 <- (2) corrupt stack
9e30390c 9193c677 win32k!xxxReceiveMessage+0x480
9e303960 9193c5cb win32k!xxxRealSleepThread+0x90
9e30397c 918ecbac win32k!xxxSleepThread+0x2d
9e3039f0 9192c3af win32k!xxxInterSendMsgEx+0xb1c
9e303a40 9192c4f2 win32k!xxxSendMessageTimeout+0x13b
9e303a68 918fbec1 win32k!xxxSendMessage+0x28
9e303b2c 91910c1a win32k!xxxCalcValidRects+0x462 <- (1) send WM_NCCALCSIZE
9e303b90 91911056 win32k!xxxEndDeferWindowPosEx+0x126
9e303bb0 918b1f89 win32k!xxxSetWindowPos+0xf6
9e303bdc 918b1ee1 win32k!xxxMoveWindow+0x8a
```

Lack of proper message locking between win32k!xxxCalcValidRects and win32k!SfnINOUTNCCALCSIZE

The exploit populates lParam with pointers to the shellcode and after being successfully copyied to kernel inside win32k!SfnINOUTNCCALCSIZE, the kernel jumps to the user level. The exploit found in the wild only targeted 32-bit versions of Windows 7.

BSOD on an up-to-date version of Windows 7 with our proof of concept

As always, we provided Microsoft with a proof of concept for this vulnerability along with well-written source code.

MICROSOFT WINDOWS | PROOF-OF-CONCEPT | VULNERABILITIES AND EXPLOITS | ZERO-DAY VULNERABILITIES

Share post on:

IN THE SAME CATEGORY


Assessing the impact of protection from web miners

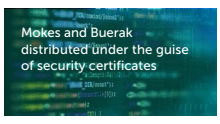

Agent 1433: remote attack on Microsoft SQL Server


How to steal a million (of your data)


On the IoT road: perks, benefits and security of moving smartly


How we hacked our colleague's smart home

Related Posts


Mokes and Buerak distributed under the guise of security certificates


Kaspersky Security Bulletin 2019. Statistics


Windows 0-day exploit CVE-2019-1458 used in Operation WizardOpium

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

SUBMIT

I'm not a robot reCAPTCHA Privacy - Terms