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

SL securelist.com/a-new-exploit-for-zero-day-vulnerability-cve-2018-8589/88845/

Research

Research

14 Nov 2018

minute read

Authors

- Expert Boris Larin
- Expert Anton Ivanov
- Expert Vladislav Stolyarov

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:

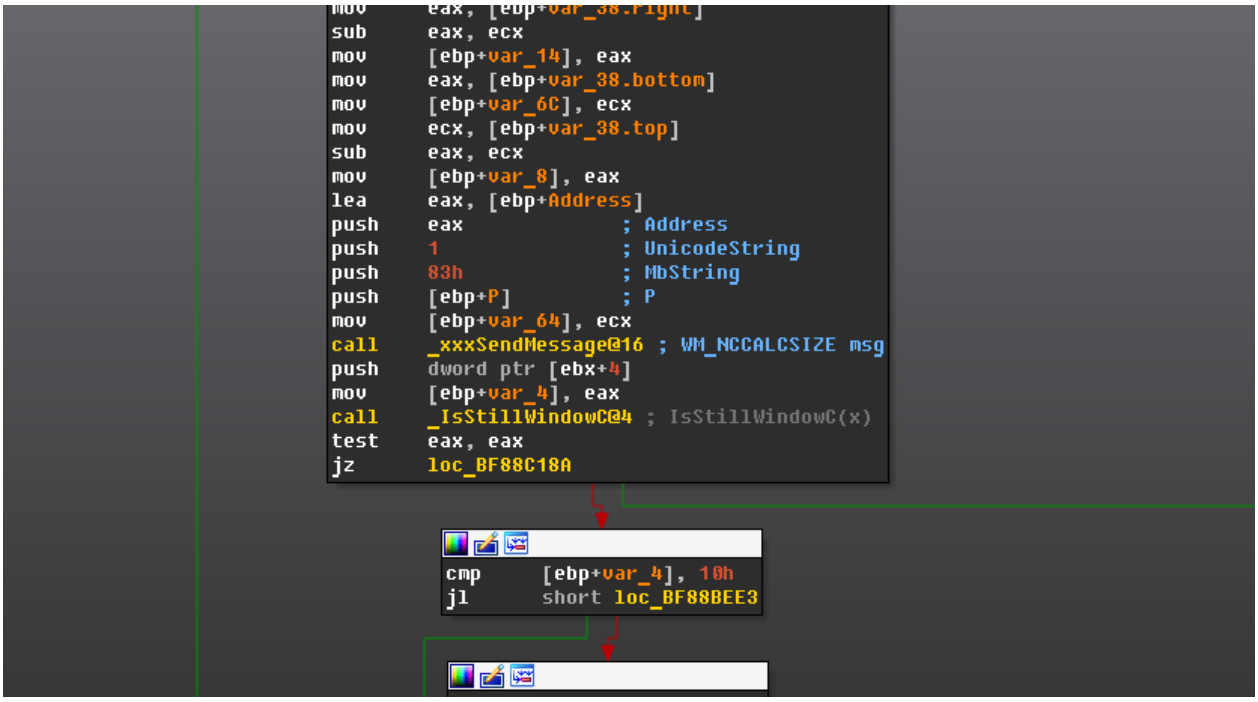
- HEUR:Exploit.Win32.Generic
- HEUR:Trojan.Win32.Generic
- PDM:Exploit.Win32.Generic

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.



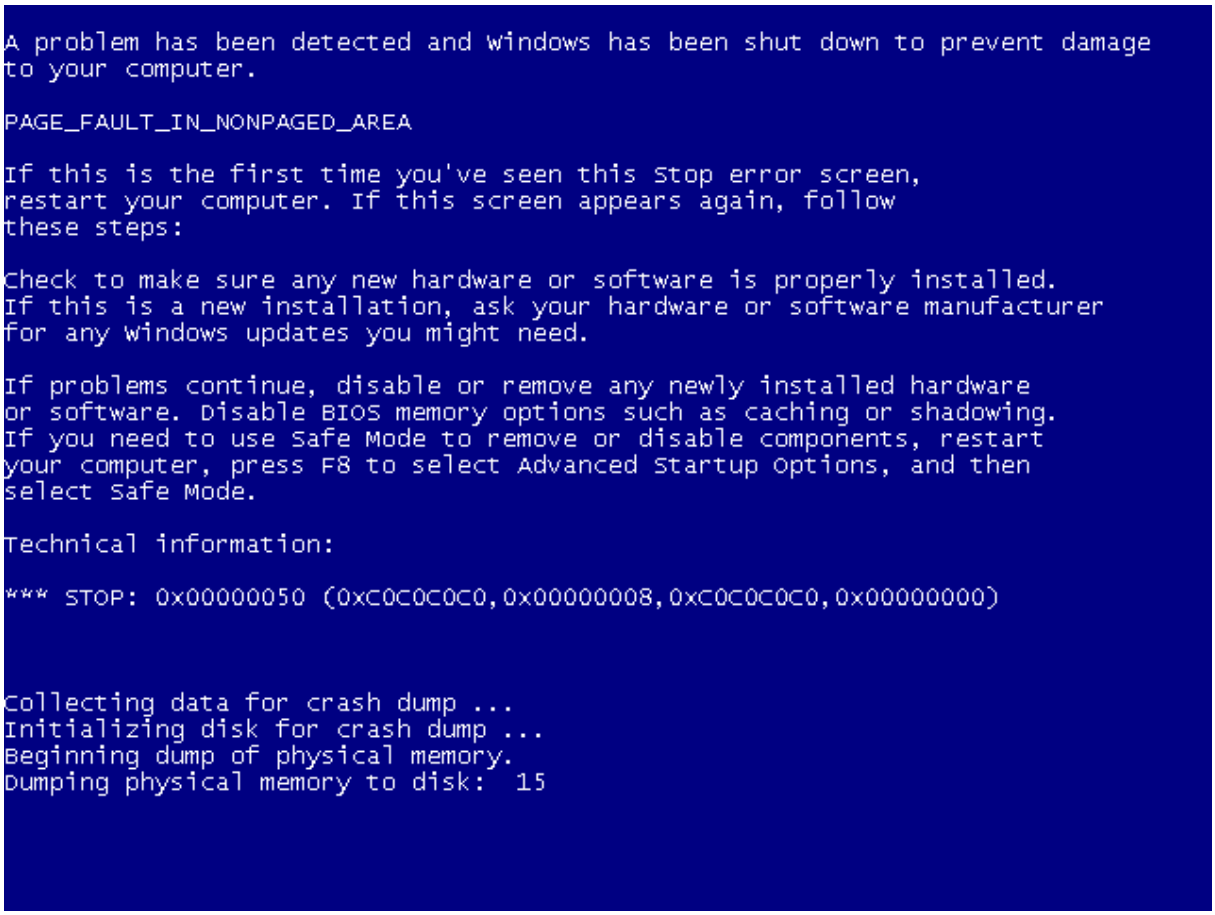
WM_NCCALCSIZE message in win32k!xxxCalcValidRects

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

Authors

- Expert Boris Larin
- Expert Anton Ivanov

- Expert Vladislav Stolyarov

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

Your email address will not be published.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

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

MysterySnail attacks with Windows zero-day

Zero-day vulnerability in Desktop Window Manager (CVE-2021-28310) used in the wild

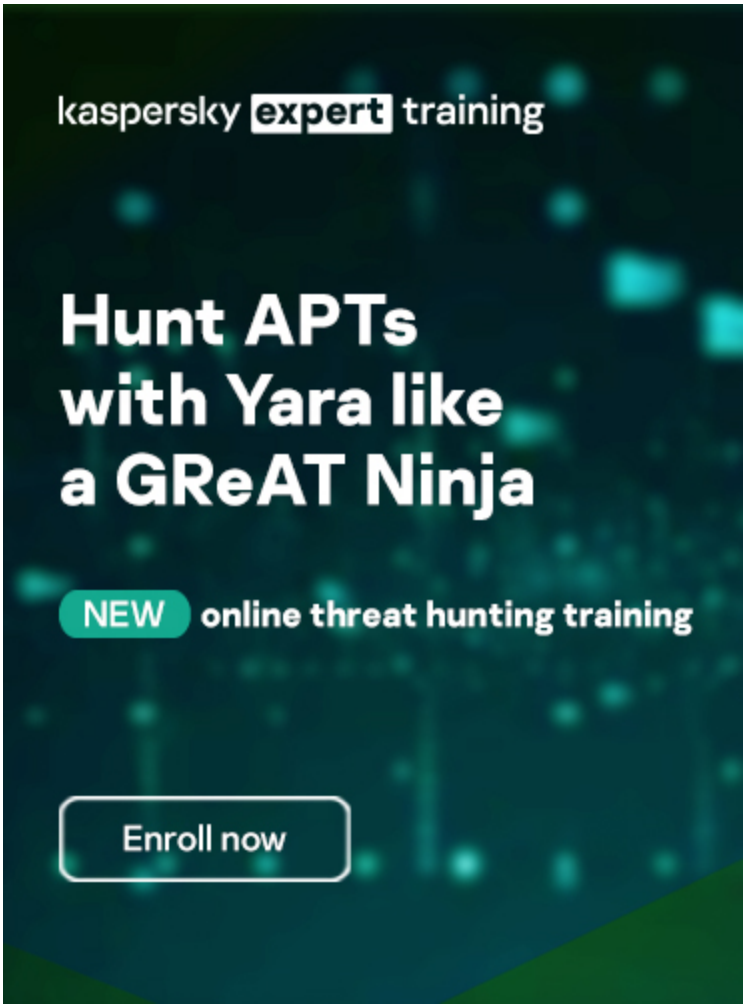
Operation PowerFall: CVE-2020-0986 and variants

Internet Explorer and Windows zero-day exploits used in Operation PowerFall

GReAT thoughts: Awesome IDA Pro plugins

Subscribe to our weekly e-mails

The hottest research right in your inbox



Reports

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.

Lazarus Trojanized DeFi app for delivering malware

We recently discovered a Trojanized DeFi application that was compiled in November 2021. This application contains a legitimate program called DeFi Wallet that saves and manages a cryptocurrency wallet, but also implants a full-featured backdoor.

MoonBounce: the dark side of UEFI firmware

At the end of 2021, we inspected UEFI firmware that was tampered with to embed a malicious code we dub MoonBounce. In this report we describe how the MoonBounce implant works and how it is connected to APT41.

The BlueNoroff cryptocurrency hunt is still on

It appears that BlueNoroff shifted focus from hitting banks and SWIFT-connected servers to solely cryptocurrency businesses as the main source of the group's illegal income.

-
-
-