Threat Groups SandCat, FruityArmor Exploiting Microsoft Win32k Flaw

By Lindsey O'Donnell

Published: 2019-03-13 · Archived: 2026-04-05 23:03:27 UTC

Newly patched CVE-2019-0797 is being actively exploited by two APTs, FruityArmor and SandCat.

A newly-patched Microsoft Win32k vulnerability is being exploited in the wild by at least two threat actors, including a recently discovered advanced persistent threat (APT) group dubbed SandCat.

The exploited vulnerability (CVE-2019-0797), rated important, was patched on Tuesday as part of Microsoft's regularly scheduled March security update. But Kaspersky Lab researchers said that the vulnerability is already being used by two APTs, SandCat and FruityArmor, to run arbitrary code on target systems.

SandCat is an APT that was discovered only recently, researchers Vasiliy Berdnikov and Boris Larin said in a Wednesday deep dive analysis of the vulnerability and its exploits.

"SandCat is a relatively new APT group; we first observed them in 2018, although it would appear they have been around for some time," Costin Raiu, director of global research and analysis team at Kaspersky Lab, told Threatpost. "They use both FinFisher/FinSpy [spyware] and the CHAINSHOT framework in attacks, coupled with various zero-days. Targets of SandCat have been mostly observed in Middle East, including but not limited to Saudi Arabia."

Meanwhile, the FruityArmor APT group is an under-the-radar cyber-espionage gang also active in the Middle East, which has been around for some time, Raiu said. FruityArmor has been known to exploit other zero days, including one (CVE-2018-8453) back in October 2018.

"The earliest publication from our side on them is from 2016, when we identified another zero day (CVE-2016-3393) being used by this group," Raiu told Threatpost. "Victims of FruityArmor are generally located in Middle East, but they are known to target journalists and activists in other regions as well."

The new exploit found in the wild is targeting 64-bit operating systems in the range from Windows 8 to Windows 10 build 15063.

"As we can see from the zero-day used in the wild, exploitation of this vulnerability is not difficult and is reliable for 64-bit operating systems in the range from Windows 8 to Windows 10 build 15063," Kaspersky Lab's Larin told Threatpost.

Both Mideast-focused APTs are selectively choosing their targets, researchers said.

"We observed very few attempts to exploit this vulnerability, in targeted attacks," Raiu told Threatpost. "This is generally the case with high-profile zero-days, which are used only for high-value targets in what can be considered surgical campaigns."

The Vulnerability

CVE-2019-0797 is an elevation of privilege vulnerability, which exists in Windows when the Win32k component fails to properly handle objects in memory. Win32k is the Windows kernel driver.

Specifically, the flaw is a race condition that is present in the win32k driver due to a lack of proper synchronization between undocumented system calls (NtDCompositionDiscardFrame and NtDCompositionDestroyConnection), researchers said. A race condition occurs when system attempts to perform two or more operations at the same time.

To exploit this, an attacker could first execute the system calls NtDCompositionDiscardFrame and NtDCompositionDestroyConnection simultaneously.

When this happens, the system call NtDCompositionDiscardFrame will look for a frame to release. During that time, the attacker would execute the function DiscardAllCompositionFrames; This condition leads to a use-after-free scenario, which is a type of memory-corruption flaw that can be leveraged by hackers to execute arbitrary code.

That means an attacker who successfully exploits this vulnerability could run arbitrary code in kernel mode – and could then install programs; view, change, or delete data; or create new accounts with full user rights.

"An attacker could…run a specially crafted application that could exploit the vulnerability and take control of an affected system," according to Microsoft's advisory.

Importantly, to exploit the vulnerability, an attacker would first have to log on to the system.

Researchers reported the flaw to Microsoft on Feb. 22. Microsoft's subsequent update, released on Patch Tuesday, addresses the vulnerability by correcting how Win32k handles objects in memory.

Don't miss our free live Threatpost webinar, "Exploring the Top 15 Most Common Vulnerabilities with HackerOne and GitHub," on Wed., Mar 20, at 2:00 p.m. ET.

Vulnerability experts Michiel Prins, co-founder of webinar sponsor HackerOne, and Greg Ose, GitHub's application security engineering manager, will join Threatpost editor Tom Spring to discuss what vulnerability types are most common in today's software, and what kind of impact they would have on organizations if exploited.
