Microsoft Offers Analysis of Zero-Day Exploited By Zirconium Group

By Tom Spring

Published: 2017-03-28 · Archived: 2026-04-05 13:13:55 UTC

Microsoft patched a zero-day vulnerability actively used in a campaign by a hacking group known as Zirconium.

Microsoft has released technical details on a zero-day vulnerability being exploited by a little-known APT group known as Zirconium. According to the company the vulnerability (CVE-2017-0005) affects mostly older versions of Windows and can allow an adversary to execute remote code if a user either visits a specially crafted website or opens a rigged document.

The vulnerability, outlined Monday in a technical paper by Microsoft, affects the Windows Win32k component in the Windows GDI (Graphics Device Interface). If exploited it could potentially allow an adversary to launch an elevation of privilege attack.

“Attackers are not as much focusing on legacy systems but avoiding security enhancements present in modern hardware and current platforms like Windows 10 Anniversary Update,” according to Matt Oh, a member of Microsoft’s Windows Defender ATP Research Team, who authored the report.

The GDI library vulnerability was patched on March 14 with MS17-013. At the time, Microsoft did not disclose the vulnerability was being actively exploited however. The bug discloses data through memory and was revealed by Google’s engineer Mateusz Jurczyk. Microsoft originally patched the vulnerability (CVE-2017-0038) in June 2016 classifying it as important. But in February, Google’s Project Zero security researchers discovered the fix was incomplete.

After skipping February’s round of Patch Tuesday updates, the company has released additional insights into the vulnerability.

A technical breakdown of the exploit by Microsoft revealed the zero-day EoP exploit targets computers running Windows 7 and Windows 8. According to researchers, there are four execution stages of the exploit package and corresponding functions.

Stage 1 is decrypting the initial main exploit code’s PE file using AES-256 algorithm. A hard-coded password is used as a key to decrypt the loader for the next stage. State 2 includes the API resolution routine, resembling, as Microsoft notes, how shellcode or position-independent code works. State 3 includes determining the identity of the operating system platform and version number.

The actual exploit routine comprises stage 4.

“After the environmental checks, the attacker code begins actual exploit of the Windows kernel vulnerability CVE-2017-0005, resulting in arbitrary memory corruption and privileged code execution,” Oh wrote.

Interesting to researchers, is the code execution used by Zirconium is made possible by a corrupted pointer in the PALETTE.pfnGetNearestFromPalentry function, which is designed to execute code in the kernel courtesy of a malformed PALETTE object. This, according to Oh, is an exploitation technique Microsoft security researchers have been tracking closely for years.

“Observed in an unrelated sample used during the Duqu incident, we have described this relatively old exploit technique in a Virus Bulletin 2015 presentation,” Oh wrote. Duqu attackers were believed to be behind attacks against certificate authorities and spy campaigns on Iran’s nuclear program.

Microsoft said, while the use of a malformed PALETTE object ties Duqu and Zirconium exploits together, however the way they take advantage of the vulnerability is different.

“This difference clearly indicates that these two exploits are unrelated, despite similarities in their code—similarities that can be attributed to the fact that these exploitation techniques are well-documented,” Oh said.

In fact, it’s the corrupted pointer in the PALETTE.pfnGetNearestFromPalentry function that Microsoft has based mitigation around CVE-2017-0005 on. In August 2016, with the Windows 10 Anniversary Update, Microsoft released tactical mitigations designed to prevent the abuse of pfnGetNearestFromPalentry, the company claims.

On the flip side of tactical mitigation are strategic mitigation efforts that include Supervisor Mode Execution Prevention (SMEP), supported by newer model Intel CPUs, and virtualization-based security (VBS).

“Strategic mitigation like SMEP can effectively raise the bar for a large pool of attackers by instantly rendering hundreds of EoP exploits ineffective, including old-school exploitation methods that call user-mode shellcode directly from the kernel, such as the zero-day exploit for CVE-2017-0005,” Oh wrote.

In some instances, Microsoft acknowledges, that sophisticated attackers have been able to work around SMEP protections.

“These bypass mechanisms include the use of kernel ROP gadgets or direct PTE modifications through read-write (RW) primitives,” he said.

To address these bypass mechanisms Microsoft said it made improvements to Windows kernel 64-bit memory-protection process ASLR it introduced with Windows 10 Anniversary Update. ASLR coupled with the OS makes SMEP stronger via randomized kernel addresses, mitigating a bypass vector resulting from direct PTE corruption, the company said.

“While patches continue to provide single-point fixes for specific vulnerabilities, this attacker behavior highlights how built-in exploit mitigations like SMEP, the ASLR improvements, and virtualization-based security are providing resiliency,” Oh said.

Oh claims Microsoft is continuing to actively research Zirconium, the APT group it identified as actively exploiting the CVE-2017-0005 vulnerability.
