Google team reveals zero-day Windows exploit

2 November 2020, by Peter Grad

Credit: Pixabay/CC0 Public Domain

Google reported a new zero-day vulnerability in Windows Friday that allows for privilege escalation and sometimes resulted in a crash. The vulnerability is a buffer overflow type in a driver found in Windows versions 7 and newer.

Google's Project Zero team said the bug, CVE-2020-17087, was being used jointly with an exploit uncovered earlier last week in Google Chrome and Chrome OS. Attackers were able to escape the confines of Chrome's sandbox and trigger an attack on the operating system.

Google fixed the Chrome vulnerability and has alerted Microsoft to the remaining bug.

A zero-day vulnerability is a fault in a system that is disclosed but not yet patched by the manufacturer.

Project Zero normally discloses vulnerabilities after 90 days or earlier if a solution is made available. But in this instance, because the bug is under active exploit and no patch has yet been issued, the Google team provided Microsoft with a seven-day window to fix the problem before it was made public.

In a post issued Friday, the Project Zero group stated: "The Windows Kernel Cryptography Driver (cng.sys) exposes a DeviceCNG device to user-mode programs and supports a variety of IOCTLs with non-trivial input structures. It constitutes a locally accessible attack surface that can be exploited for privilege escalation (such as sandbox escape)."

Microsoft has not yet resolved the problem. Google says it expect Microsoft to issue a patch on November 10, the second Tuesday of the month that is traditionally when Microsoft dispatches accumulated patches.

Microsoft has offered no guidance on addressing the issue until a patch is released. But a company representative said there is no evidence the bug is being widely exploited.

In a statement released last week, Microsoft said: "Microsoft has a customer commitment to investigate reported security issues and update impacted devices to protect customers. While we work to meet all researchers' deadlines for disclosures, including short-term deadlines like in this scenario, developing a security update is a balance between timeliness and quality, and our ultimate goal is to help ensure maximum customer protection with minimal customer disruption."

Shane Huntley, director of Google's Threat Analysis team, said the attacks were targeted and are not related to Tuesday's presidential election.

Attackers manipulated a function in the Windows Kernel Cryptography Driver by inserting a number into a buffer that is below an allowable level. When the number is converted to a hexadecimal from a binary, input/output controllers can be hijacked to transmit data into a secure area that allows code execution, providing the attacker with access to the

system outside of the protected sandbox.

The Chrome flaw resolved late last month resided in the FreeType font-rendering library.

More information:
bugs.chromium.org/p/project-ze … ssues/detail?id=2104

APA citation: Google team reveals zero-day Windows exploit (2020, November 2) retrieved 18 June 2021 from https://techxplore.com/news/2020-11-google-team-reveals-zero-day-windows.html