UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00066

ZERO-DAY MICROSOFT KERNAL FLAW

DATE ISSUED: 10th November 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Under active exploitation in the wild, this local privilege escalation attack and subsequent sandbox escape has been disclosed by Google's Project Zero team before a patch has become available. CVE-2020-17087

BREAKDOWN

Windows Kernel Cryptography Driver (cng.sys) that is responsible for processing system call input and output controls (IOCTLs) exposes \DNG\CNG devices to user-mode programs which support numerous IOCTLs and leave IOCTL 0x390400 reachable through a series of calls. Attackers can use arbitrary requests to trigger pool-based buffer overflows resulting in systems crashing and becoming vulnerable to exploitation. The exploit occurs in tandem with the Google Chrome flaw CV-2020-15999 and appears to be highly targeted. This attack can result in privilege escalation and potential sandbox escape.

Google's Project Zero team formulated a Proof of Concept (PoC) scenario using Windows 10 v1903 64bit to demonstrate the ease of this attack's execution. A patch is expected to be released in Microsoft's next batch release of security updates this week.

REMEDIATION STEPS

- Install security patches issued by Microsoft in the coming days according to normal process
- Ensure Google Chrome is the latest version to prevent this attack-chain exploit
- Use endpoint protection and detection technologies to respond to suspicious local activity

REFERENCES & RESOURCES

Threatpost https://threatpost.com/unpatched-windows-zero-day-exploited-sandbox-escape/160828/
Helpnet Security https://www.helpnetsecurity.com/2020/11/02/cve-2020-17087/