Google discloses a zero-day bug in Windows affecting Windows 7 and Windows 10

Google has disclosed a zero-day bug in the Windows OS with an extreme severity rating. The security researchers said that hackers are actively utilizing the vulnerability. The team has disclosed the vulnerability along with a distinct zero-day vulnerability in Chrome. Google has disclosed and patched this bug last week in Chrome version 86.0.4240.111.

What is Vulnerability?

The vulnerability works in coordination with the Chrome vulnerability which permits hackers to run malicious code inside Chrome. The Windows bug was used in the second division of the attack where hackers could run a malicious piece of code on the primary Windows operating system escaping the system privileges and Chrome security. Such an attack is called the “Sandbox escape” by the experts.

The Windows Kernel Cryptography Driver shows a CNG device to user-mode programs and provides various IOCTL(s) (system calls for device-specific input/output operations). It forms a locally reachable attack surface that can be exploited for Sandbox Escape.

CVE-2020-17087 is the vulnerability ID that allows hackers to escalate system rights. Another zero-day vulnerability tracked as CVE-2020-15999 to lead the malicious attacks. This vulnerability has a high severity rating and affects all Windows versions between Windows 7 and the newly released Windows 10 version.

Project Zero (P0), a team of security analysts created by Google to find a zero-day vulnerability reveals bugs periodically. Google gave Microsoft the deadline of seven days to fix the security fault. Microsoft has planned to fix this flaw by November 10.

According to Google, Chinese government-backed hackers acted as the staff from cybersecurity provider McAfee and deceived users into installing malware into their system. Google’s Threat Analysis Group (TAG) that works on stopping cyber attacks identified the action and sent out a warning and also shared the verdicts with the Federal Bureau of Investigation (FBI).