

**Windows Zero-Day CVE-2020-17087**

MS19810638 –H.W.Y.K Geethanjana Offensive Hacking: Tactical & Strategic IE6052

M.Sc. (Specialized in Cyber Security)

Sri Lanka Institute of Information Technology

Contents

[**Windows Zero-Day CVE-2020-17087** 0](file:///F:\MSC\MSC%204th%20sem\CVE%20report\Microsoft%20Windows%20Kernel%20Zero-Day%20Vulnerability-CVE-2020-17087.docx#_Toc73043562)

[1. Introduction 0](#_Toc73043563)

[2. Vulnerability 1](#_Toc73043564)

[2.1 Challenges 1](#_Toc73043565)

[2.2 Affected areas and related vulnerabilities 1](#_Toc73043566)

[2.3 Support and Mitigation 2](#_Toc73043567)

[3. Patching and maintaining 3](#_Toc73043568)

[4. Conclusion 4](#_Toc73043569)

[References 5](#_Toc73043570)

# 1. Introduction

The Windows zero-day elevation of privileges (EoP) vulnerability **CVE-2020-17087** is being actively exploited in the wild and likely affects Win 7 and higher systems. More technical information has been provided in the Chromium issue tracker [entry](https://bugs.chromium.org/p/project-zero/issues/detail?id=2104), which was kept inaccessible to the wider public for the first seven days, but has now been made public.The researchers have also included PoC exploit code, which has been tested on Windows 10 1903 (64-bit), but they noted that the affected driver (cng.sys) “looks to have been present since at least Windows 7,” meaning that all the other supported Windows versions are probably vulnerable.[1]

According to Ben Hawkes, team lead for Project Zero, Google's elite vulnerability testing team, the zero-day is supposed to be fixed on November 10, which is the date of the next Microsoft Release Tuesday.On Twitter, Hawkes said the zero-day Windows (tracked as CVE-2020-17087) was used along with another zero-day Chrome as part of a two-punch attack (tracked as CVE-2020-15999)[1]The zero-day Chrome was used to encourage attackers to execute malicious code within Chrome, while the second component of this assault was the zero-day Windows, allowing threat actors to escape the protected container of Chrome and run code on the underlying operating system, in what security practitioners term a sandbox escape. Microsoft was alerted last week by the Google Project Zero team[2] who gave the company seven days to fix the error. Information was released today as a patch was not released by Microsoft at the allotted time.

**WINDOWS 7 TO WINDOWS 10 ARE IMPACTED**

The zero-day is a bug in the Windows kernel, according to Google's report, that can be abused with additional permissions to elevate an attacker's code.

The vulnerability affects all versions of Windows between Windows 7 and the new Windows 10 update, per the report.Also included was proof of the principle code to replicate attacks.Hawkes did not provide any specifics as to who was using these two zero-days. Nation-sponsored hacker groups or large cybercrime groups typically discover most zero-days.

The attacks were also verified by a second Google security unit, Google's Threat Detection Department, according to the same Google article (TAG).

The attacks are not linked to the US election, Shane Huntley, Google TAG Operator, said. In Chrome update 86.0.4240.111, Chrome Zero-Day was patched.[3] This is the second time Google has unveiled a two-pronged assault featuring a zero-day Windows and Chrome attack. In March 2019, Google said threat actors have mixed a zero-day Chrome (CVE-2019-5786) with a zero-day Windows (CVE-2019-0808).[2]

# 2. Vulnerability

The zero-day, dubbed CVE-2020-17087, was revealed on October 30 by the Google Project Zero and TAG security teams. The vulnerability was used in conjunction with a Chrome zero-day to target Windows 7 and Windows 10 users, according to Google. Around mid-October, Google uncovered the zero-day and gave Microsoft seven days to release a patch. Because it takes time to test and fine-tune a security patch for any Microsoft product—especially the bulky Windows OS—the patch was not available during the intended seven-day disclosure schedule.

The zero-day is located in the Windows kernel and affects all presently supported versions of the Windows OS, according to Microsoft's security warning for CVE-2020-17087. All versions of Windows after Windows 7 are included,[3] as well as all Windows Server deployments.

Apart from the Windows zero-day, there are 111 additional flaws that need to be fixed, including 24 problems in Excel, Microsoft Sharepoint, Microsoft Exchange Server, the Windows Network File System, the Windows GDI+ component, the Windows printing spooler service, and even Microsoft Teams.While installing updates quickly is safe for most users, system administrators of big networks should test the patches before deploying them widely to eliminate any flaws or modifications that disrupt internal systems.

## 2.1 Challenges

Google's Project Zero offers proof-of-concept code as well. We can simply leverage the kernel encryption driver to create system crashes with the aid of proof-of-concept code. The kernel encryption driver (cng.sys) is an essential component of Windows. When an exception occurs, this driver may trigger a blue screen of death. Microsoft has received a vulnerability report, according to Google's Project Zero, and will remedy the issue in Windows 10 with a security update delivered on November 10.

This vulnerability, however, also affects the Windows 7 and Windows Server 2008 operating systems. These versions are no longer available and will not be updated.

## 2.2 Affected areas and related vulnerabilities

**CVE-2020-17087 | Local Elevation of Privilege Vulnerability in the Windows Kernel**

CVE-2020-17087 is an elevation of privilege vulnerability in the Windows kernel Cryptography Driver, cng.sys, that was exploited in the wild in conjunction with CVE-2020-15999, a buffer overflow vulnerability in Google Chrome's FreeType 2 library. CVE-2020-17087 was used to bypass Google Chrome's sandbox, allowing the exploited system to gain elevated privileges. This is the second vulnerability chain exploited in the last year, this time involving a Google Chrome flaw and a Windows elevation of privilege flaw.[4]

Threat actors use vulnerability chaining to their advantage. While both CVE-2020-15999 and CVE-2020-17087 have been exploited in the wild as zero-days, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI published a joint advisory last month that highlighted threat actors chaining unpatched vulnerabilities to gain initial access and elevate privileges in a target environment. Now that Google and Microsoft have patched these flaws, it's critical for businesses to make sure they've installed the updates before threat actors start using them more widely.

**CVE-2020-17051 | Remote Code Execution Vulnerability in the Windows Network File System**

The Windows Network File System is affected by CVE-2020-17051, a critical remote code execution (RCE) vulnerability (NFS). NFS is a file system protocol that allows multiple operating systems on a network to share files.[4]

According to the limited information provided by Microsoft, the vulnerability appears to affect all supported versions of Windows and, based on the CVSSv3 score of 9.8, can be exploited without authentication or user interaction. According to a McAfee blog post, combining CVE-2020-17051 with CVE-2020-17056, a remote kernel data read vulnerability in NFS, could increase the likelihood of a remote exploit by bypassing address space layout randomization (ASLR). CVE-2020-17051 may also be wormable, according to the blog post, if NFS is configured to allow anonymous write access. We recommend that businesses prioritize updates for both of these CVEs, as Microsoft has labeled this vulnerability as "Exploitation More Likely" on its Exploitability Index.

**CVE-2020-17083 and CVE-2020-17084 | Remote Code Execution Vulnerability in Microsoft Exchange Server**

RCE weaknesses CVE-2020-17083 and CVE-2020-17084 exist in Microsoft Exchange Server. CVE-2020-17083 has a CVSSv3 score of 5.5, whereas CVE-2020-17084 has an 8.5.[4] Despite the fact that both issues are listed as "Exploitation Less Conceivable," based on the CVSS score, it's likely that both vulnerabilities might be exploited by luring a user into opening a prepared email. Steven Seeley of Source Incite is to blame for the flaws. While not proven, these changes are most likely related to a bypass discovered by Seeley for CVE-2020-16875. On Twitter, Seeley pointed out that the CVSS score for CVE-2020-17083 is erroneous, and that it should be 8.5. Over the years, attackers have found Microsoft Exchange to be an attractive target,[4] and sluggish patching of Exchange servers has resulted in successful assaults against corporations. CVE-2020-0688 was the subject of active investigation immediately after the patch was published in February of this year.

## 2.3 Support and Mitigation

Microsoft will provide enhanced security support to fix the vulnerability unless enterprise users have already purchased Microsoft's paid extended support plan.If possible, users who are still using an old version of the operating system that has been discontinued should upgrade as soon as possible to a supported operating system. In reaction to Google's early disclosure of the information of the unpatched vulnerabilities, Microsoft executives responded as well. This time, Microsoft's attitude appears to be more restrained.

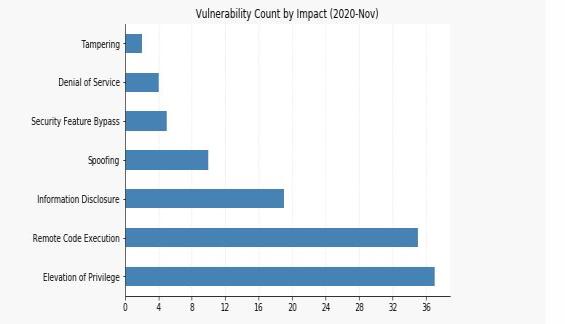
Microsoft is committed to investigating security vulnerabilities reported by researchers as quickly as possible, while also releasing security updates as quickly as possible to address related vulnerabilities and protect customers.

While balancing the timeliness of security updates and development quality, Microsoft will strive to meet all researchers' disclosure deadlines.

According to a Microsoft spokesperson, the vulnerability is being used in a very limited and targeted way, and the company has no evidence that it is being widely exploited.

# 3. Patching and maintaining

Shane Huntley, Director of Google’s Threat Analysis Group (TAG) confirmed that the vulnerability chain is being used for targeted exploitation and that the attacks are “not related to any US election-related targeting.”

The attackers are using the Chrome bug to gain access to the target system and then the CVE-2020-17087 to gain administrator access on it.A patch for the issue is expected to be released on November 10, as part of the monthly Patch Tuesday effort by Microsoft. While the bug is serious, the fact that it’s being used in targeted (and not widespread) attacks should reassure most users they’ll be safe until the patch is released. Also, according to a Microsoft spokesperson, exploitation of the flaw has only been spotted in conjunction with the Chrome vulnerability, which has been patched [in Chrome](https://chromereleases.googleblog.com/2020/10/stable-channel-update-for-desktop_20.html) and other Chromium-based browsers (e.g., [Opera](https://blogs.opera.com/desktop/2020/10/opera-72-update/) on October 21, [Microsoft Edge](https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV200002) on October 22.[5]

Security-Only patches for operating systems that provide a Monthly Rollup or Security-Only update streams do not include browser remediation. Organizations opting for Security-Only patches[6] should be aware that there are separate Cumulative Security Updates for Internet Explorer.

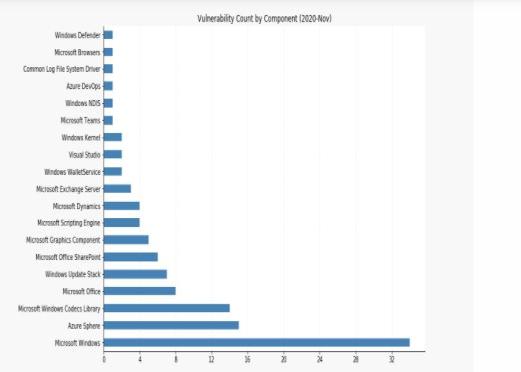


Figure 1: Vulnerability count by component (2020 Nov.)

Figure 2 : Vulnerability count by impact (2020 Nov.)

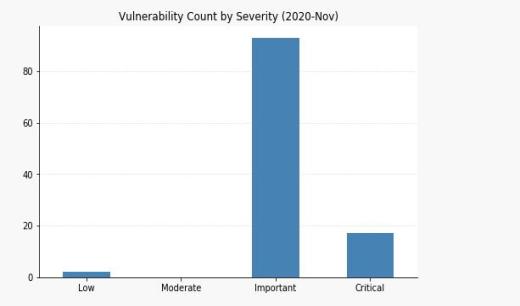


Figure 3 : Vulnerability count by severity (2020 Nov.)

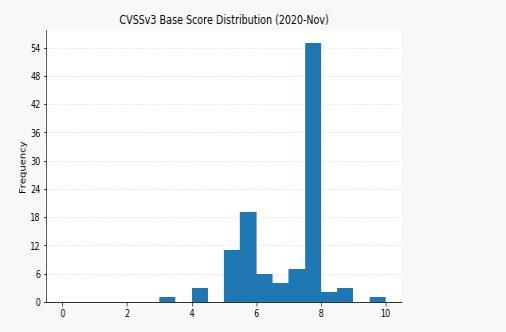


Figure 4 : CVSSV3 base Score Distribution (2020 Nov.)

Note: Graph data is reflective of data presented by Microsoft's CVRF

# 4. Conclusion

**CVE-2020-17087**

The flaw is in the Windows kernel cryptography driver (cng.sys), which results in a buffer overflow that may be used to get elevated privileges. The Windows Kernel Cryptography Driver (cng.sys) exposes a DeviceCNG device to user-mode applications and supports a variety of IOCTLs (input-output control interfaces) with non-trivial input forms. It creates a locally accessible attack surface that may be used to escalate privileges.

**Impact**

The zero-day vulnerability in Chrome has already been patched by Google. The remote execution is not deemed to harm users who have installed Chrome's fix, while it is still feasible to execute locally.

**The affected version of windows**

The bug is expected to affect Windows 7 through Windows 10.

**Solution**

**SanerNow** offers the detection and remediation for CVE-2020-15999. It can also detect the affected Windows OS for CVE-2020-17087. Patch for the same is currently unavailable from Microsoft[6].

According to the tweet by Ben Hawkes, the patch for CVE-2020-17087 is expected to be released on November 10 (Patch Tuesday).

While the flaw is significant, the fact that it's only being utilized in targeted (rather than widespread) assaults should reassure most users that they'll be secure until a fix is published. According to a Microsoft spokesman, the problem was only discovered in conjunction with the Chrome vulnerability, which was patched in Chrome and other Chromium-based browsers As a result, users who have installed such updates are even safer.

# References

[1] BOB HUBER, “Patch Tuesday, November 2020 Edition.” [Online]. Available: https://krebsonsecurity.com/2020/11/patch-tuesday-november-2020-edition/.

[2] Maddie Stone, “Project Zero.” [Online]. Available: https://googleprojectzero.blogspot.com/2021/03/in-wild-series-october-2020-0-day.html.

[3] Aditya Saroha, “Google discloses new zero-day vulnerability in Windows OS.” [Online]. Available: https://www.thehindu.com/sci-tech/technology/google-discloses-new-zero-day-vulnerability-in-windows-os/article33001875.ece.

[4] Security Response Team-Tenable, “Microsoft’s November 2020 Patch Tuesday Addresses 112 CVEs including CVE-2020-17087,” *Security Response Team | Research Tanable*. [Online]. Available: https://www.tenable.com/blog/microsoft-s-november-2020-patch-tuesday-addresses-112-cves-including-cve-2020-17087.

[5] M. E. Zeljka Zorz, “Google discloses actively exploited Windows zero-day (CVE-2020-17087).” [Online]. Available: https://www.helpnetsecurity.com/2020/11/02/cve-2020-17087/.

[6] A. Bisht, “Google Discloses Windows Zero-Day Vulnerability Being Exploited in the Wild.” [Online]. Available: https://www.secpod.com/blog/windows-zero-day-vulnerability-being-exploited-in-the-wild-cve-2020-17087/.