BIZCOMMUNITY

# 4 security vulnerabilities found in Microsoft Office

Cyber threat intelligence company Check Point Research (CPR) has discovered four security vulnerabilities that affect products in Microsoft Office, including Excel and Office online.

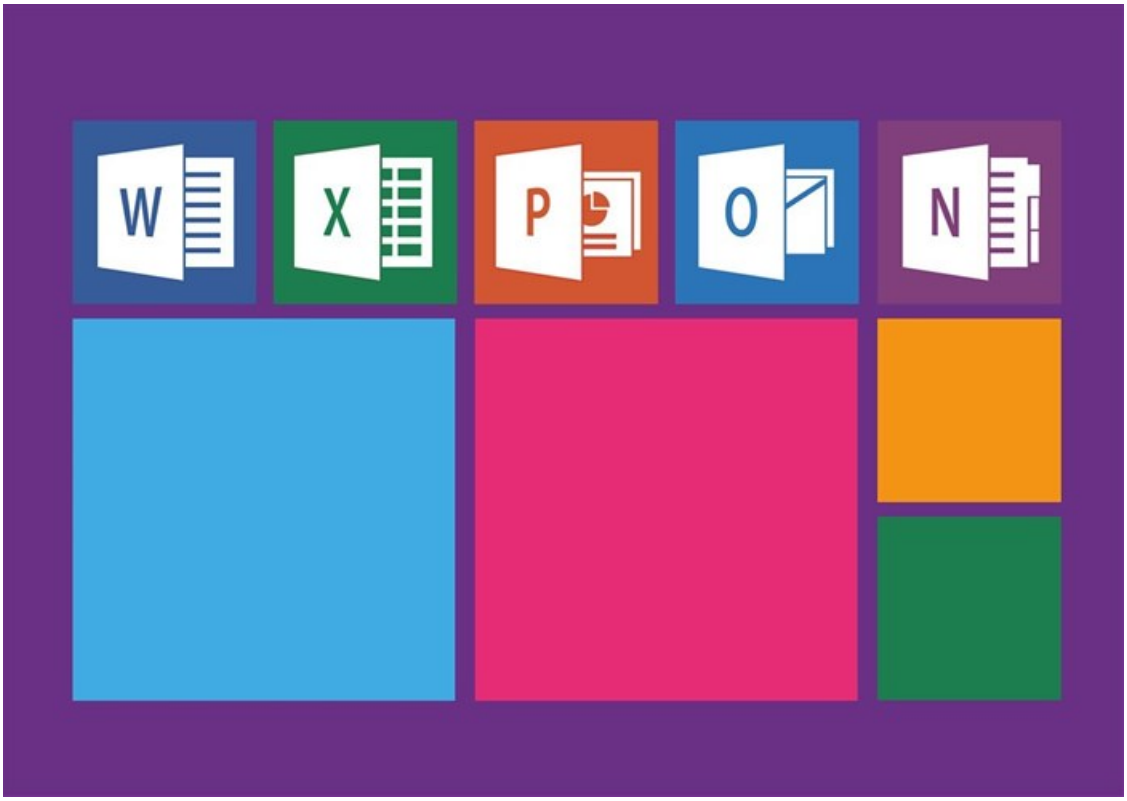

Image by Pixaline from Pixabay

CPR said the vulnerabilities are rooted in legacy code and could have granted an attacker the ability to execute code on targets via malicious Office documents, such as Word, Excel and Outlook. The vulnerabilities are the result of parsing mistakes made in legacy code found in Excel95 File Formats, giving researchers reason to believe that the security flaws have existed for several years.

## Discovery

CPR discovered the vulnerabilities by “fuzzing” MSGraph, a component that can be embedded inside Microsoft Office products in order to display graphs and charts. Fuzzing is an automated software testing technique that attempts to find hackable software bugs by randomly feeding invalid and unexpected data inputs into a computer programme in order to find coding errors and security loopholes.

By using the technique, CPR discovered vulnerable functions inside MSGraph. Similar code checks confirmed that the vulnerable function was commonly used across multiple different Microsoft Office products, such as Excel, Office Online Server, and Excel for OSX.

## Attack methodology

The vulnerabilities found can be embedded in most Office documents. Hence, there are multiple attack vectors that can be imagined. The simplest one would be:

- A victim downloads a malicious Excel file (XLS format). =The doc can be served via a download link or an email, but

the attacker cannot force the victim to download it.
- The victim opens the malicious Excel file.
- The vulnerability is triggered.

Since the entire Office suite has the ability to embed Excel objects, this broadens the attack vector, making it possible to execute such an attack on almost any Office software, including Word, Outlook and others.

## Disclosure

CPR disclosed its research finding to Microsoft. Microsoft patched the security vulnerabilities, issuing CVE-2021-31174, CVE-2021-31178, CVE-2021-31179. The fourth patch will be issued on Microsoft's Patch Tuesday on June 8, 2021, classified as (CVE-2021-31939).

Yaniv Balmas, head of cyber research at Check Point Software, said: "The vulnerabilities found affect almost the entire Microsoft Office ecosystem. It's possible to execute such an attack on almost any Office software, including Word, Outlook and others. We learned that the vulnerabilities are due to parsing mistakes made in legacy code."

"One of the primary learnings from our research is that legacy code continues to be a weak link in the security chain, especially in complex software like Microsoft Office. Even though we found only four vulnerabilities on the attack surface in our research, one can never tell how many more vulnerabilities like these are still lying around waiting to be found. I strongly urge Windows users to update their software immediately, as there are numerous attack vectors possible by an attacker who triggers the vulnerabilities that we found."

> *We have recently discovered 4 security issues applicable in most MS-Office products.*
>
> *Read all the details here:https://t.co/KxPiOnCxeq*
> *cc @sagitz_ @NetanelBenSimon— Check Point Research (@_CPResearch_) June 8, 2021*