# Microsoft patches vulnerability in Windows AppX Installer being used to spread Emotet malware

Microsoft has patched a critical zero-day vulnerability in Windows that is being exploited by cybercriminals to spread Emotet malware.

This vulnerability, tracked under code CVE-2021-43890, is related to Windows AppX Installer spoofing. Cybercriminals can remotely exploit this vulnerability with low user privileges. However, for successful exploitation, it is necessary to organize attacks of high complexity and require user (victim) interaction.

"We investigated reports of a rogue vulnerability in AppX Installer affecting Microsoft Windows. Microsoft discovered attacks attempting to exploit this vulnerability with specially crafted software packages. especially, including the famous Emotet malware," Microsoft shared.

According to Microsoft, hackers will create an attachment containing malicious code to use in phishing campaigns. Next, the hacker will spread this attachment in spam emails with content that entices users to open them.

## How to not be affected by Windows AppX Installer vulnerability?

To prevent hackers, Windows users need to install a patched version of Microsoft Desktop Installer on their platform:

1. Microsoft Desktop Installer 1.16 for Windows 10 version 1809 or later
2. Microsoft Desktop Installer 1.11 for Windows 10 version 1709 or 1803

Microsoft also provides mitigations for customers who are unable to immediately install Microsoft Desktop Installer updates.

Those measures include enabling BlockNonAdminUserInstall to prevent non-Administrator users from installing Windows App packages and AllowAllTrustedAppToInstall to block installs from apps outside of the Microsoft Store.