Security Advisory 2021-069

Windows AppX Installer Spoofing Vulnerability

December 15, 2021 — v1.0

TLP:WHITE

History:

- *15/12/2021 — v1.0 – Initial publication*

Summary

On December 14th, Microsoft released an advisory [2] to address a Windows AppX Installer spoofing security flaw tracked as CVE-2021-43890. It can be exploited remotely by threat actors with low user privileges in high complexity attacks requiring user interaction [1]. Attacks attempting to exploit this vulnerability has been already observed in the wild.

Technical Details

Microsoft investigated reports of a spoofing vulnerability in AppX installer that affects Microsoft Windows. *Microsoft is aware of attacks that attempt to exploit this vulnerability by using specially crafted packages that include the malware family known as Emotet/Trickbot/Bazaloader*. [2]

According to Microsoft, an attacker could craft a malicious attachment to be used in phishing campaigns. The attacker would then have to convince the user to open the specially crafted attachment. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights [2].

BleepingComputer previously reported that Emotet began spreading using malicious Windows App Installer packages camouflaged as Adobe PDF software. While Microsoft did not directly link the CVE-2021-43890 zero-day to this campaign, the details from yesterday's advisory line up with tactics used in recent Emotet attacks.

Recommendations

Microsoft has patched this high severity Windows zero-day vulnerability. CERT-EU recommends to install the patched Microsoft Desktop Installer:

- Microsoft Desktop Installer 1.16 for Windows 10, version 1809 and later;
- Microsoft Desktop Installer 1.11 for Windows 10, version 1709 or Windows 10, version 1803.

Workarounds

- Enable `BlockNonAdminUserInstall` GPO to prevent non-admins from installing any Windows App packages.
- Enable `AllowAllTrustedAppToInstall` GPO to prevent installing apps from outside the Microsoft Store.
- Use Windows Defender Application Control or AppLocker to block the Desktop App Installer app (`Microsoft.DesktopAppInstaller_8wekyb3d8bbwe`), or create policies to limit the apps installed in your environment.
- Disable the `ms-appinstaller` protocol to install apps directly from a website.

References

[1] https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-appx-installer-zero-day-used-by-emotet/

[2] https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-43890