Hive Pro

THREAT ADVISORY

Microsoft released patch for actively exploited spoofing vulnerability

TA202159

Threat Level AMBER

Publish Date – Dec 16, 2021

Microsoft AppX has a spoofing vulnerability that has been assigned CVE-2021-43890. Attackers are taking advantage of this critical vulnerability by deploying well-known malwares such as Emotet, Trickbot, and Bazaloader.

This vulnerability allows an attacker to create a malicious package file and modify it to look like a legitimate application and then convince the victim to open it, which will then execute code and allow to gain access to the victim's machine.

The TTPs that might be used by an unknown attacker includes:
TA0001 - Initial Access
T1566 - Phishing
T1566.001 - Phishing: Spearphishing Attachment
T1189 - Drive-by Compromise
TA0002 - Execution
T1204 - User Execution
T1204.002 - User Execution: Malicious File
TA0005 - Defense Evasion
T1036 - Masquerading
T1036.005 - Masquerading: Match Legitimate Name or Location
T1574 - Hijack Execution Flow
TA0003 - Persistence
TA0004 - Privilege Escalation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-43890	Microsoft App Installer	cpe:2.3:a:microsoft:app_installer:*:*:*:*:*:*:*:*	Windows AppX Installer Spoofing Vulnerability	CWE-20, CWE-345

Patch Links

https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43890

References

https://thehackernews.com/2021/12/microsoft-issues-windows-update-to.html
https://vuldb.com/?id.188264