CVE-2021-43890

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2021-43890
State	PUBLIC
Assigner	secure@microsoft.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-12-15 15:15:00 UTC
Updated	2023-12-30 07:15:00 UTC
Description	Windows AppX Installer Spoofing Vulnerability

Risk And Classification

EPSS: 0.164370000 probability, percentile 0.949000000 (date 2026-04-29)

CISA KEV: Listed on 2021-12-15; due 2021-12-29; ransomware use Known

Problem Types: NVD-CWE-noinfo

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows AppX Installer Spoofing Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2021-43890

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	App Installer	All	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All
Operating System	Microsoft	Windows 10	-	All	All	All

References

Reference	Source	Link
Security Update Guide - Microsoft Security Response Center	MISC	portal.msrc.microsoft.com
Microsoft disables MSIX protocol handler abused in malware attacks		www.bleepingcomputer.c
Microsoft Disables MSIX App Installer Protocol Widely Used in Malware Attacks		thehackernews.com

Microsoft Disables MSIX App Installer Protocol Widely Used in Malware Attacks		thehackernews.com
Added Winget Check and Install by mrhaydendp · Pull Request #26 · ChrisTitusTech/winutil · GitHub		github.com
Financially motivated threat actors misusing App Installer | Microsoft Security Blog		www.microsoft.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

91848 Windows AppX Installer Spoofing Vulnerability

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**