



Microsoft Windows Installer Vulnerability

Windows Installer Zero-Day actively being exploited by malware

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379>
CVEs: CVE-2021-41379

Exploitation of the vulnerability could lead to attackers having sytem privileges running the latest Windows releases, including Windows 10, Windows 11, and Windows Server 2022.

Background	Microsoft announced a vulnerability on Windows Installer as part of their Patch Tuesday. A security researcher discovered that the patch was not enough and have posted a proof of concept.
Announced	November 9, 2021, Microsoft announced a privilege escalation vulnerability on Windows Installer.
Latest Developments	on December 20, 2021, Security researcher Abdelhamid Naceri posted a proof of concept further exploiting the already-patched Windows Installer. Based on FortiGuard statistics from the last few days, Malware using this vulnerability is active in the wild.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Weaponization

Delivery

AV

Blocks exploitation of malware related to Windows Installer Vulnerability (CVE-2021-41379)

FortiGate

DB 89.07141

FortiWeb

DB 89.07141

FortiClient

DB 89.07141

FortiSASE

DB 89.07141

FortiMail

DB 89.07141

FortiCASB

DB 89.07141

FortiCWP

DB 89.07141

FortiADC

DB 89.07141

FortiProxy

DB 89.07141

AV (Pre-filter)

Blocks exploitation of malware related to Windows Installer Vulnerability (CVE-2021-41379)

FortiEDR

DB 89.07141

FortiSandbox

DB 89.07141

Exploitation

IPS

Blocks exploitation of Windows Installer Vulnerability (CVE-2021-41379)

FortiGate

DB 18.204

FortiSASE

DB 18.204

FortiNDR

DB 18.204

FortiADC

DB 18.204

FortiProxy

DB 18.204

Installation

C2

Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer

DB 1.00035

Threat Hunting

FortiAnalyzer

v6.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training

Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Additional Resources

Microsoft	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379
Bleeping Computer	https://www.bleepingcomputer.com/news/security/malware-now-trying-to-exploit-new-windows-installer-zero-day/
Threat Post	https://threatpost.com/attackers-target-windows-installer-bug/176558/
The Hacker News	https://thehackernews.com/2021/11/warning-hackers-exploiting-new-windows.html

Learn more about [FortiGuard Outbreak Alerts](#)

FORTINET