F#RTINET. **OUTBREAK ALERTS** 

# 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

11, and Windows Server 2022.

Microsoft announced a vulnerability on Windows Installer as part of their Patch Tuesday. A security researcher

Exloitation of the vulnerability could lead to attackers having sytem privileges running the latest Windows releases, including Windows 10, Windows

discovered that the patch was not enough and have posted a proof of concept.

November 9, 2021, Microsoft announced a privilege escalation vulnerability on Windows Installer.

**Latest Developments** 

already-patched Windows Installer. Based on FortiGuard statistics from the last few days, Malware using this vulnerability is active in the wild.

on December 20, 2021, Security researcher Abdelhamid Naceri posted a proof of concept further exploiting the

**FortiMail** 

DB 89.07141

**FortiCASB** 

DB 89.07141

DB 89.07141



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

**PROTECT** 

events: Reconnaissance

**FortiSASE** 

DB 89.07141

**Delivery** 

AV

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



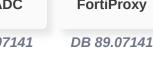
**FortiGate** 



DB 89.07141

**FortiClient** 

DB 89.07141

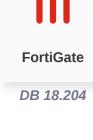






## **Blocks exploitation of Windows Installer Vulnerability (CVE-2021-41379)**

**FortiProxy** 













## alert and generate reports:

DETECT

**Outbreak Detection** 

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



**FortiAnalyzer** 

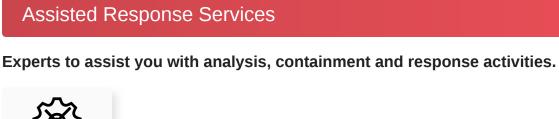




## **Automated Response** Services that can automatically respond to this outbreak.

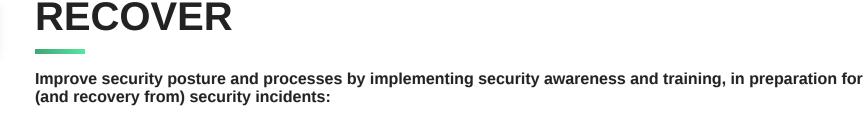
**RESPOND** 

Develop containment techniques to mitigate impacts of security events:



**FortiXDR** 

### Incident Response



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

**NOC/SOC Training** 

Response

Readiness

**End-User Training** 

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download



**NSE Training** 



# **IDENTIFY**

Attack Surface Hardening

and other forms of cyberattacks.

Identify processes and assets that need protection:

**Security** Rating

https://thehackernews.com/2021/11/warning-hackers-exploiting-new-windows.html

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

**Additional Resources** 

Learn more about FortiGuard Outbreak Alerts

#### 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/ https://threatpost.com/attackers-target-windows-installer-bug/176558/



**Threat Post** 

**The Hacker News** 





Weaponization

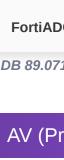


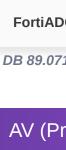


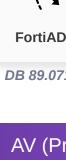






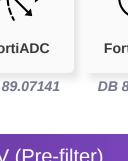






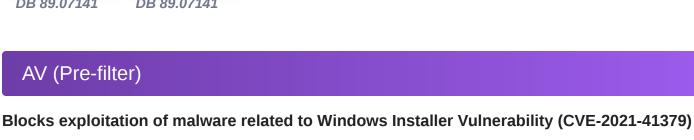




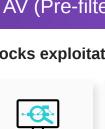




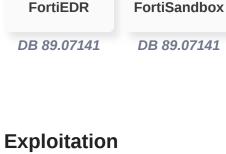






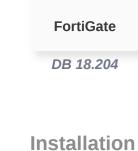










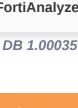














v6.4+

