F#RTINET.

OUTBREAK ALERTS

MSDT DogWalk Vulnerability





Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution **Vulnerability**

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-34713 CVEs: CVE-2022-34713

August patch Tuesday from Microsoft introduced fixes for 121 vulnerabilities. Of these, two are zero-day fixes, and one -- CVE-34713 a.k.a. 'DogWalk' -- is being actively exploited in the wild.

Background

A remote code execution vulnerability exists when Microsoft Windows MSDT is called using the URL protocol from a calling application. Successful exploitation of this vulnerability could allow an attacker to deploy a malicious executable into the Windows Startup folder. Administrators and users of affected products are advised to upgrade

Announced

to the latest versions immediately. Aug 4, 2022: Microsoft determined that this issue meets the criteria for servicing with a security update; tagging it

Latest Developments

Aug 9, 2022: Microsoft released the fix via August 'Patch Tuesday' update.



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

PROTECT

as CVE-2022-34713.

Reconnaissance

Weaponization

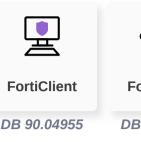
Delivery

AV

Blocks malware exploiting the MSDT "DogWalk" RCE vulnerability (CVE-2022-34713).







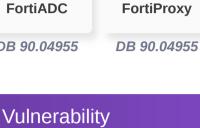












Detects systems vulnerable to the MSDT "DogWalk" Remote Code Execution Vulnerability, and auto-patches when

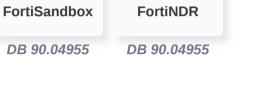


FortiClient

Exploitation

FortiEDR

DB 90.04955

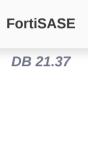


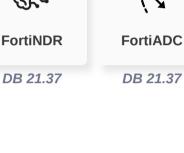
Blocks attack attempts related to MSDT "DogWalk" RCE vulnerability (CVE-2022-34713).

IPS

DB 21.37 DB 21.37









Action

C2

Threat Hunting

DETECT

alert and generate reports:

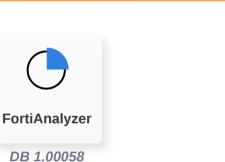
FortiAnalyzer

v7.0+

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



FortiEDR





Services that can automatically respond to this outbreak.

Assisted Response Services

Automated Response

RESPOND

FortiXDR

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

Develop containment techniques to mitigate impacts of security events:



RECOVER

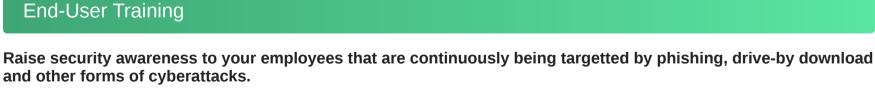
(and recovery from) security incidents:

Response

Readiness

NOC/SOC Training Train your network and security professionals and optimize your incident response to stay on top of the

Improve security posture and processes by implementing security awareness and training, in preparation for



Security

Training

cyberattacks.

NSE Training

Awareness &



Security

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

Rating **Vulnerability Management**

Attack Surface Hardening

Reduce the attack surface on software vulnerabilities via systematic and automated patching.

FortiEDR

https://thehackernews.com/2022/08/microsoft-issues-patches-for-121-flaws.html

The Hacker News

Threat Signal

Additional Resources

Bleeping Computer https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-windows-dogwalk-zero-day-exploited-in-attacks/

https://www.fortiguard.com/threat-signal-report/4704

Learn more about FortiGuard Outbreak Alerts