

## 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 to the latest versions immediately.
Announced	Aug 4, 2022: Microsoft determined that this issue meets the criteria for servicing with a security update; tagging it as CVE-2022-34713.
Latest Developments	Aug 9, 2022: Microsoft released the fix via August 'Patch Tuesday' update.


## PROTECT


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


- Reconnaissance
- Weaponization
- Delivery


### AV


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


  
FortiGate  
DB 90.04955


  
FortiWeb  
DB 90.04955


  
FortiClient  
DB 90.04955


  
FortiSASE  
DB 90.04955

  
FortiMail  
DB 90.04955

  
FortiCASB  
DB 90.04955


  
FortiCWP  
DB 90.04955

  
FortiADC  
DB 90.04955

  
FortiProxy  
DB 90.04955


### Vulnerability


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


  
FortiClient  
DB 1.332

### AV (Pre-filter)

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

  
FortiEDR  
DB 90.04955


  
FortiSandbox  
DB 90.04955


  
FortiNDR  
DB 90.04955


## Exploitation


### IPS


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

  
FortiGate  
DB 21.37

  
FortiSASE  
DB 21.37

  
FortiNDR  
DB 21.37

  
FortiADC  
DB 21.37


  
FortiProxy  
DB 21.37


- Installation
- C2
- Action

## DETECT


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

### Threat Hunting

  
FortiEDR

  
FortiAnalyzer  
v7.0+

### Outbreak Detection


  
FortiAnalyzer  
DB 1.00058

## 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

### Vulnerability Management

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

  
FortiEDR

## Additional Resources

The Hacker News	<a href="https://thehackernews.com/2022/08/microsoft-issues-patches-for-121-flaws.html">https://thehackernews.com/2022/08/microsoft-issues-patches-for-121-flaws.html</a>
Bleeping Computer	<a href="https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-windows-dogwalk-zero-day-exploited-in-attacks/">https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-windows-dogwalk-zero-day-exploited-in-attacks/</a>
Threat Signal	<a href="https://www.fortiguard.com/threat-signal-report/4704">https://www.fortiguard.com/threat-signal-report/4704</a>

Learn more about [FortiGuard Outbreak Alerts](#)