OUTBREAK ALERTS

MSDT Follina Vulnerability

A 0-day Windows MSDT Vulnerability

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
CVEs: CVE-2022-30190

A vulnerability on Microsoft Support Diagnostic Tool (MSDT) in Microsoft Windows has been spotted in the wild that allows remote code execution.

Background	A cybersecurity researcher from nao_sec spotted a vulnerability on a Microsoft Word document uploaded in VirusTotal. The document abuses the MSDT URI scheme to download and run malicious payload. The document references "0438" which is an area code for Follina municipality in Italy.
Announced	May 30, 2022: Microsoft released a security update at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190
Latest Developments	May 30, 2022: Microsoft posted a guidance at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190 May 30, 2022: The Hacker News published an article at https://thehackernews.com/2022/05/watch-out-researchers-spot-new.html

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiWeb
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiClient
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

Vulnerability 1.320
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiEDR
AV (Pre-Filter) 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiSASE
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiSandbox
AV (Pre-Filter) 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiNDR
AV (Pre-Filter) 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

ANN 1.100
Blocks malware exploiting using AI/ML.

FortiMail
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiCASB
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiCWP
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiADC
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

FortiProxy
AV 90.02802
Blocks malware exploiting the MSDT RCE vulnerability (CVE-2022-30190).

Exploitation

FortiGate
IPS 20.326
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiClient
Application Firewall 21.328
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiSASE
IPS 20.326
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiNDR
IPS 20.326
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiADC
IPS 20.326
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

FortiProxy
IPS 20.326
Blocks attack attempts related to MSDT RCE vulnerability (CVE-2022-30190).

Installation

FortiEDR
Post-Execution 4.0+
Detects post-exploitation behavior associated with the CVE-2022-30190 vulnerability.

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiAnalyzer

Outbreak Detection Version 1.056
https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00056

Threat Hunting Version 7.0+
https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-Follina-Microsoft/ta-p/213558

FortiSIEM

Threat Hunting Version 6.5
https://help.fortinet.com/fsiem/6-5-0/Online-Help/HTML5_Help/content_updates.htm#Content2

Additional Resources

CISA Gov	https://www.cisa.gov/uscert/ncas/current-activity/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability
Threat Signal	https://www.fortiguard.com/threat-signal-report/4603/follina-0-day-windows-msdt-vulnerability-cve-2022-30190-exploited-in-the-wild