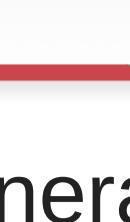




OUTBREAK ALERTS



Microsoft 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>

PROTECT

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

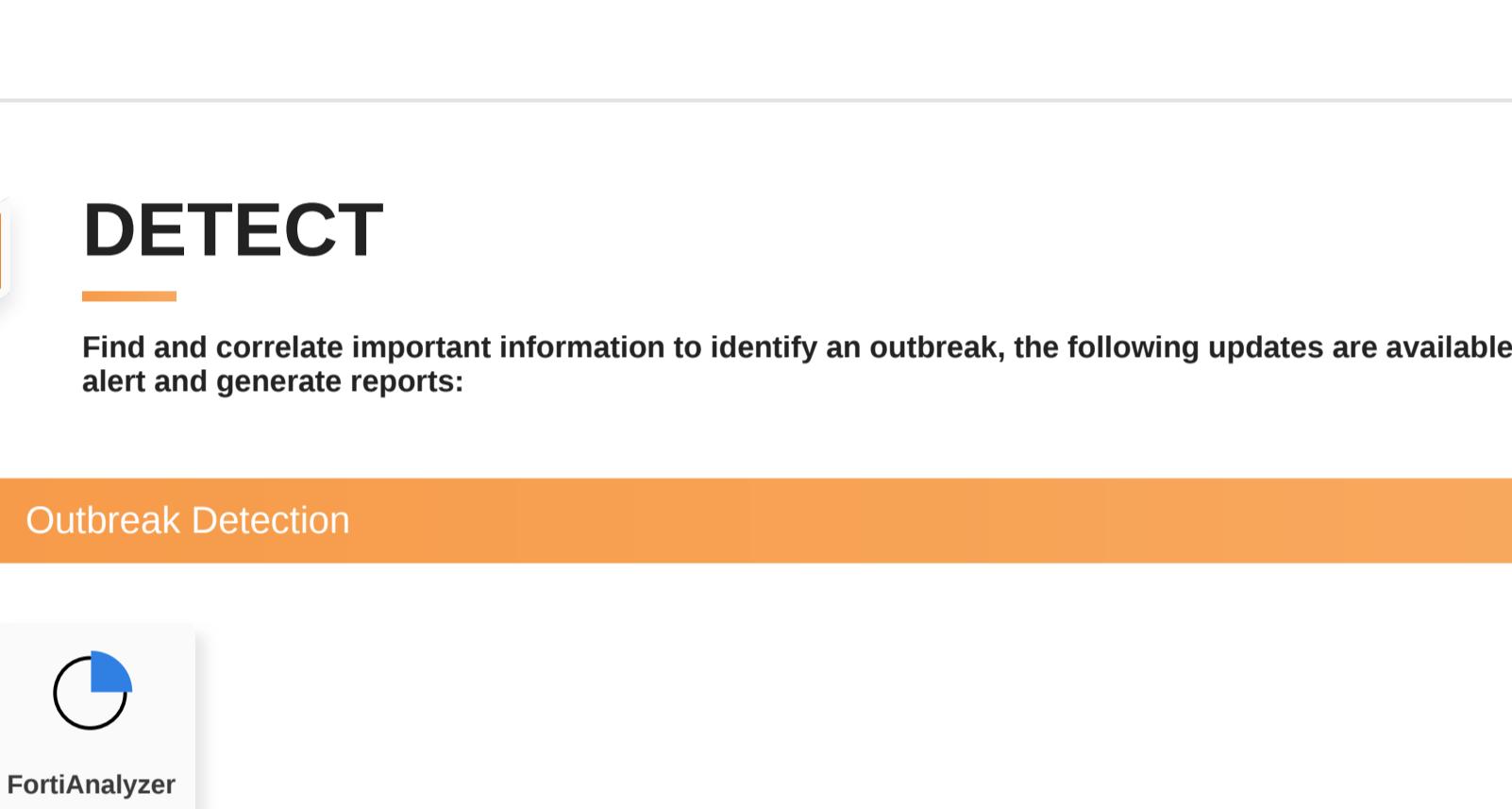
Reconnaissance

Weaponization

Delivery

AV

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



AV (Pre-filter)

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



Exploitation

IPS

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



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



Threat Hunting



Content Update



RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

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

RECOVER

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

NOC/SOC Training

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

End-User Training

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

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

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

Learn more about [FortiGuard Outbreak Alerts](#)

Learn more about [FortiGuard Outbreak Alerts](#)