



# OUTBREAK ALERTS



## Microsoft WinHTTP Protocol Stack RCE Vulnerability

A remote code execution vulnerability in Windows' Internet Information Services (IIS) component.

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21907>

CVEs: [CVE-2022-21907](#)

Microsoft's January 2022 Patch Tuesday contains updates on 97 security vulnerabilities, one of which is CVE-2022-21907 rated with 9.8 and can lead to a remote code execution.

### Background

As reported by Microsoft - during the January 2022 security update cycle - a patch was released for vulnerabilities CVE-2022-21907. That is a critical bug on HTTP Protocol Stack that can lead to a remote code execution without any user interaction or privilege required.

### Announced

On January 11, the Microsoft security update was published at:

<https://msrc.microsoft.com/update-guide/releaseNote/2022-Jan>

And, a cybersecurity news site ThreatPost published a follow-up article at:  
<https://threatpost.com/microsoft-wormable-critical-rce-bug-zero-day/177564>

On January 12, FortiGuard Labs published a threat signal report:  
<https://www.fortiguard.com/threat-signal-report/4372>

### Latest Developments

FortiGuard Labs is actively monitoring for detections in the wild. Refer the table below for the latest Security Fabric protections available

## PROTECT

undefined

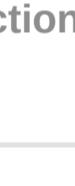
Reconnaissance

Weaponization

Delivery

Vulnerability

Detects the presence of the HTTP Protocol Stack RCE vulnerability, and applies auto-patching if enabled.



FortiClient

DB 1.287

Exploitation

IPS

Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability



FortiGate

DB 19.241



FortiSASE

DB 19.241



FortiNDR

DB 19.241



FortiADC

DB 19.241



FortiProxy

DB 19.241

Web App Security

Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability



FortiWeb

DB 0.00311



FortiADC

DB 1.32

Application Firewall

Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability



FortiClient

DB 19.242

Installation

C2

Action

## DETECT

undefined

Outbreak Detection

Detects indicators for the HTTP Protocol Stack RCE vulnerability across the Security Fabric



FortiAnalyzer

DB 1.00048

Threat Hunting

Detects indicators for the HTTP Protocol Stack RCE vulnerability across the Security Fabric



FortiAnalyzer

v6.4+

InfoSec Services

Assisted Response Services

Incident Response



FortiRecon AEM

FortiRecon AEM

## RESPOND

undefined

Automated Response

undefined



FortiXDR

Assisted Response Services

undefined



FortiRecon AEM

Incident Response



FortiRecon AEM

FortiRecon AEM

## RECOVER

undefined

InfoSec Services

undefined



Response Readiness

InfoSec Services

undefined

## IDENTIFY

undefined

Attack Surface Monitoring (Inside & Outside)

undefined



Security Rating



FortiEAM

FortiEAM

