Windows HTTP Protocol Stack RCE

RCE in Windows HTTP Protocol Stack

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.

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*19.241*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
FortiWeb	**Web App Security**	*0.00311*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
FortiClient	**Vulnerability**	*1.287*	Detects the presence of the HTTP Protocol Stack RCE vulnerability, and applies auto-patching if enabled.
	Application Firewall	*19.242*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
FortiADC	**IPS**	*19.241*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
	Web App Security	*1.32*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
FortiProxy	**IPS**	*19.241*	Blocks attempts to exploit the HTTP Protocol Stack RCE vulnerability
FortiAnalyzer	**Outbreak Detection**	*1.048*	Detects indicators for the HTTP Protocol Stack RCE vulnerability across the Security Fabric
	Threat Hunting	*6.4+*	Detects indicators for the HTTP Protocol Stack RCE vulnerability across the Security Fabric

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient
Vulnerability
Version Info: 1.287
Link: https://www.fortiguard.com/updates/epvuln?version=1.287

Exploitation

FortiGate
IPS
Version Info: 19.241
Link: https://www.fortiguard.com/updates/ips?version=19.241

FortiWeb
Web App Security
Version Info: 0.00311
Link: https://www.fortiguard.com/updates/websecurity?version=0.00311

FortiClient
Application Firewall
Version Info: 19.242
Link: https://www.fortiguard.com/updates/ips?version=19.242

FortiADC
IPS
Version Info: 19.241
Link: https://www.fortiguard.com/updates/ips?version=19.241

Web App Security
Version Info: 1.32
Link:

FortiProxy
IPS
Version Info: 19.241
Link: https://www.fortiguard.com/updates/ips?version=19.241

Installation

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:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
Outbreak Detection
Version Info: 1.048
Link: https://www.fortiguard.com/updates/outbreak-detection-service?version=1.00048

Threat Hunting
Version Info: 6.4+
Link: https://community.fortinet.com/t5/FortiAnalyzer/Technical-Tip-Using-FortiAnalyzer-to-detect-attempts-at/ta-p/203227