



## Microsoft Windows RPC RCE Vulnerability

### WannaCry about it later or patch it now?

<https://www.fortiguard.com/outbreak-alert/microsoft-windows-rpc-rce-vulnerability>  
 CVEs: CVE-2022-26809

This vulnerability is a critical remote code execution vulnerability in Remote Procedure Call Runtime Library. A remote, unauthenticated attacker could exploit this vulnerability to take control of an affected system.

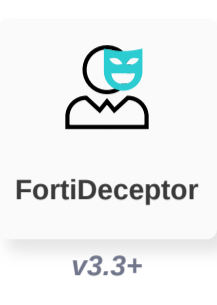
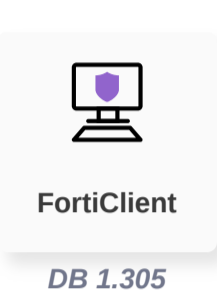
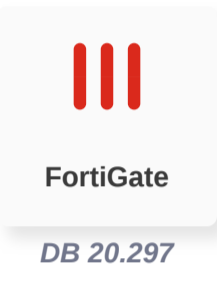

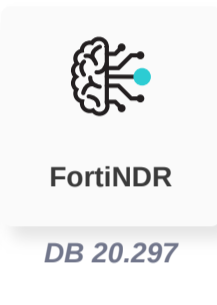
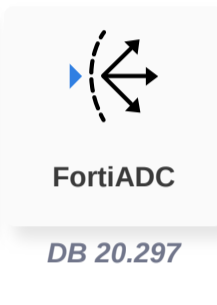

**Background** This vulnerability uses the SMB port - that means if someone were to exploit it and weaponize it with ransomware, then it could become as dangerous as WannaCry.

**Announced** April 12, 2022:  
<https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26809>

**Latest Developments** April 13, 2022: See below for more details on the product mapping. At this time, Microsoft claims there are no known exploits in the wild.

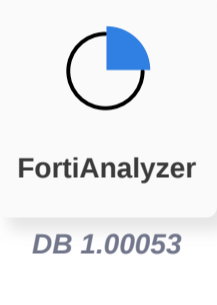
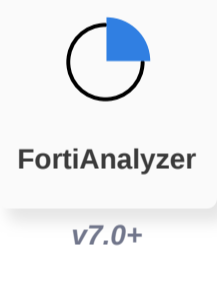
### PROTECT

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

- Reconnaissance**
  - Decoy VM**  
 FortiDeceptor decoys can detect activities related to The Microsoft Driver RCE vulnerability - CVE-2022-26809  
  
 FortiDeceptor v3.3+
- Weaponization**
- Delivery**
  - Vulnerability**  
 Detect & respond to endpoints vulnerable to the Microsoft RPC-RCE Vulnerability (CVE-2022-26809)  
  
 FortiClient DB 1.305
- Exploitation**
  - IPS**  
 Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)  
 FortiGate DB 20.297  
 FortiSASE DB 20.297  
 FortiNDR DB 20.297  
 FortiADC DB 20.297  
 FortiProxy DB 20.297
- Installation**
- C2**
- Action**

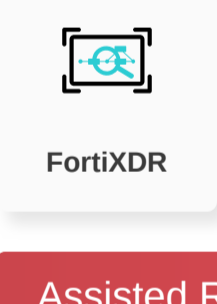
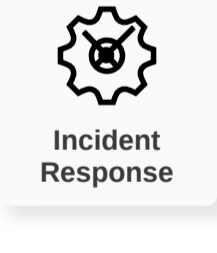
### DETECT

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

- Outbreak Detection**  
  
 FortiAnalyzer DB 1.00053
- Threat Hunting**  
  
 FortiAnalyzer v7.0+

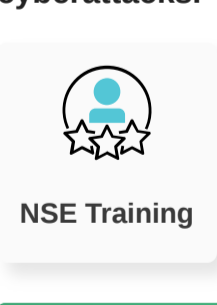


### RESPOND

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

## Additional Resources

**Threat Signal** <https://www.fortiguard.com/threat-signal-report/4502>

Learn more about [FortiGuard Outbreak Alerts](#)