Microsoft Windows RPC RCE Vulnerability

WannaCry about it later or patch it now?


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


CVEs:

CVE-2022-26809

April 13, 2022: Fortinet has coverage in both Network IPS and Endpoint Vulnerability detection for this vulnerability. See below for more details on the product mapping. At this time, Microsoft claims there are no known exploits in the wild.

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 1.0063

FortiSASE

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiProxy

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiADC

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiGate

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiClient

Vulnerability 2.257
Detect & respond to endpoints vulnerable to the Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiDeceptor

Decoy VM V3.3+
FortiDeceptor decoys can detect activities related to the Microsoft Driver RCE vulnerability (CVE-2022-26809)

FortiSOAR

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 1.0063

FortiSASE

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiProxy

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiADC

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiGate

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiClient

Vulnerability 2.257
Detect & respond to endpoints vulnerable to the Microsoft Driver RCE vulnerability (CVE-2022-26809)

FortiDeceptor

Decoy VM V3.3+
FortiDeceptor decoys can detect activities related to the Microsoft Driver RCE vulnerability (CVE-2022-26809)

Additional Resources

Microsoft Announcement

CISA Re-post
https://www.cisa.gov/uscert/ncas/current-activity/2022/04/13/microsoft-releases-advisory-address-critical-remote-code-execution

FortiGuard Threat Signal
https://www.fortiguard.com/threat-signal-report/4502

National Vulnerability DB

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 1.0063

FortiSASE

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiProxy

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiADC

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiGate

IPS - 20.297
Detect activities on exploitation of Microsoft RPC-RCE vulnerability (CVE-2022-26809)

FortiClient

Vulnerability 2.257
Detect & respond to endpoints vulnerable to the Microsoft Driver RCE vulnerability (CVE-2022-26809)

FortiDeceptor

Decoy VM V3.3+
FortiDeceptor decoys can detect activities related to the Microsoft Driver RCE vulnerability (CVE-2022-26809)