BLOG

CVE-2022-26809 REMOTE PROCEDURE CALL RUNTIME REMOTE CODE EXECUTION VULNERABILITY AND COVERAGE

SIEM

By Securonix Threat Labs

Microsoft has released an advisory to address CVE-2022-26809, CVSS score: 9.8, an RCE vulnerability in Remote Procedure Call (RPC) Runtime Library. A remote, unauthenticated attacker could exploit this vulnerability to take control of an affected system.

To prevent exploitation, Securonix recommends blocking port 445 and 135 on the enterprise firewall and per Microsoft's recommendation, secure all SMB traffic.

We advise customers to use Securonix policy "Suspicious Process Spawned By Remote Procedure Call Service" and/or the below queries to detect exploitation of this vulnerability.

Title: Suspicious Process Spawned By Remote Procedure Call Service

Description: Detects anomalous process spawned by the remote procedure call service (RPC).

Confidence: Medium

Supported Version: 6.3 and 6.4

index = activity AND rg_functionality = "Endpoint Management Systems" AND (deviceaction = "Process Create" OR deviceaction = "Process Create (rule: ProcessCreate)" OR deviceaction = "ProcessRollup2") AND sourceprocessname = "svchost.exe" AND resourcecustomfield2 CONTAINS "RPCSS" | STATS destinationprocessname

For the latest threat intelligence and updates please refer to our Github page that is updated daily. We also invite you to send your questions regarding critical security advisories to the Securonix Critical Intelligence Advisory team and look forward to being of assistance.

PREVIOUS ARTICLE
Securonix Announces Bi-Directional Integration with ServiceNow for Rapid Incident Response

NEXT ARTICLE
It's Much More Than Just One Less Tab

Related Resource

THREAT RESEARCH

Details and Guidance on New "FortiJump" Vulnerability or CVE-2024-47575

Learn More

THREAT RESEARCH

Securonix Threat Labs Monthly Intelligence Insights – September 2024

Learn More

THREAT RESEARCH

SHROUDED#SLEEP: A Deep Dive into North Korea's Ongoing Campaign Against Southeast Asia

Learn More

THREAT RESEARCH

Securonix Threat Labs Summer Intelligence Insights – 2024

Learn More