IMBAUAN KEAMANAN KERENTANAN *REMOTE PROCEDURE CALL RUNTIME REMOTE CODE EXECUTION* PADA WINDOWS 10 (CVE 2022-26809)

Ringkasan Eksekutif

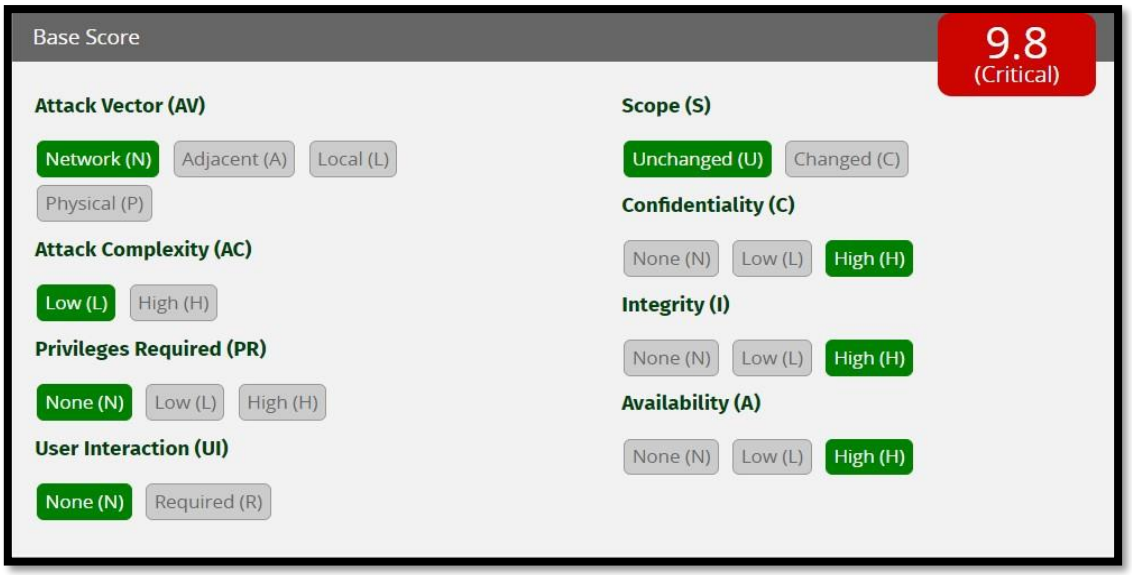
1. Pada 12 April 2022, *Microsoft Security Response Center* mengeluarkan publikasi mengenai kerentanan Remote Procedure Call Runtime Remote Code Execution.
2. Kerentanan ini dideskripsikan pada CVE 2022-26809 sebagai kerantanan yang memiliki dampak *Critical* dengan nilai 9,8.
3. Kerentanan ini terdapat pada beberapa produk dari Microsoft seperti Windows 7, Windows 8.1, Windows 10, Windows 11, Windows Server 2008, Windows Server 2016, Windows Server 2019, dan Windows Server 2022.
4. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan CVE 2022-26809, diharapkan pengguna dari produk terdampak ataupun pengguna pemerintah dan publik lainnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

Pada tanggal 12 April 2022, Microsoft Security Response Center merilis peringatan keamanan yang diidentifikasi sebagai CVE 2022-26809. Microsoft Windows merupakan sistem operasi produk dari Microsoft. Microsoft Remote Procedure Call (RPC) merupakan salah satu teknologi Microsoft yang digunakan untuk membuat program klien/server terdistribusi. Libraries dan stub. pada RPC run-time mengatur sebagian besar proses yang berhubungan dengan protokol jaringan dan komunikasi. Keberadaan RPC ini dapat mempermudah pengguna karena pengguna hanya perlu fokus pada detail aplikasi yang sedang digunakan daripada detail jaringan.

Nilai Kerentanan

Berdasarkan CVSS 3.1, CVE 2022-26809 memiliki nilai **9,8** dengan tingkat dampak **CRITICAL**.



Gambar 1. *Base Score* untuk Kerentanan CVE 2022-26809

Vector String (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Produk Terdampak

Produk yang memiliki kerentanan CVE 2022-26809 terdapat pada tabel berikut:

No	Nama Produk	No	Nama Produk
1.	Windows 7 for 32-bit Systems Service Pack 1	30.	Windows Server 2008 R2 for x64-based Systems Service Pack 1
2.	Windows 7 for 32-bit Systems Service Pack 1	31.	Windows 10 Version 20H2 for 32-bit Systems
3.	Windows Server 2016 (Server Core installation)	32.	Windows 10 Version 20H2 for x64-based Systems
4.	Windows 11 for ARM64-based Systems	33.	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
5.	Windows Server, version 20H2 (Server Core Installation)	34.	Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
6.	Windows 10 Version 20H2 for ARM64-based Systems	35.	Windows Server 2016
7.	Windows 10 Version 1909 for ARM64-based Systems	36.	Windows 10 Version 1607 for x64-based Systems
8.	Windows 10 Version 1809 for x64-based Systems	37.	Windows 10 Version 1607 for 32-bit Systems
9.	Windows 10 for 32-bit Systems	38.	Windows 10 for x64-based Systems
10.	Windows 10 Version 21H2 for x64-based Systems	39.	Windows 10 Version 1909 for x64-based Systems

11.	Windows 10 Version 21H2 for ARM64-based Systems	40.	Windows 10 Version 1909 for 32-bit Systems
12.	Windows 10 Version 21H2 for 32-bit Systems	41.	Windows 10 Version 1809 for ARM64-based Systems
13.	Windows 10 Version 1809 for 32-bit Systems	42.	Windows Server 2008 for x64-based Systems Service Pack 2
14.	Windows Server 2022 (Server Core installation)	43.	Windows Server 2008 for x64-based Systems Service Pack 2
15.	Windows Server 2022	44.	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
16.	Windows 10 Version 21H1 for 32-bit Systems	45.	Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
17.	Windows 10 Version 21H1 for ARM64-based Systems	46.	Windows 8.1 for 32-bit systems
18.	Windows 10 Version 21H1 for x64-based Systems	47.	Windows 8.1 for 32-bit systems
19.	Windows Server 2012 R2 (Server Core installation)	48.	Windows 7 for x64-based Systems Service Pack 1
20.	Windows Server 2012 R2 (Server Core installation)	49.	Windows 7 for x64-based Systems Service Pack 1
21.	Windows Server 2012 R2	50.	Windows Server 2008 for 32-bit Systems Service Pack 2
22.	Windows Server 2012 R2	51.	Windows Server 2008 for 32-bit Systems Service Pack 2
23.	Windows Server 2012 (Server Core installation)	52.	Windows RT 8.1
24.	Windows Server 2012 (Server Core installation)	53.	Windows 8.1 for x64-based systems
25.	Windows Server 2012	54.	Windows 8.1 for x64-based systems
26.	Windows Server 2012	55.	Windows 11 for x64-based Systems
27.	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	56.	Windows Server 2019 (Server Core installation)

28.	Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)	57.	Windows Server 2019
29.	Windows Server 2008 R2 for x64-based Systems Service Pack 1		

Detail dan Dampak Kerentanan

Berdasarkan perhitungan yang dilakukan, diperoleh informasi bahwa *Attack Vector* (AV) berasal dari jaringan, memiliki *Attack Complexity* (AC) yang rendah, tidak memerlukan *privilege* maupun *user interaction*. Hal ini semakin memperbesar nilai dampak karena memiliki pengertian bahwa penyerang dapat menyerang sistem tanpa membutuhkan persetujuan/interaksi dari pengguna. Selain itu, jika kerentanan ini berhasil dieksploitasi, maka akan memiliki nilai resiko yang tinggi terhadap aspek kerahasiaan, integritas, dan ketersediaan. Dampak dari kerentanan ini adalah penyerang dapat melakukan proses *Remote Code Execution* (RCE) yang memungkinkan penyerang untuk mengambil alih sistem secara utuh.

Panduan Mitigasi

Deputi Bidang Operasi Keamanan Siber dan Sandi mengimbau agar segera melakukan langkah mitigasi lebih lanjut yang direkomendasikan untuk pihak pengelola sistem informasi. Untuk melakukan pencegahan terhadap eksploitasi kerentanan CVE 2022-26809, terdapat beberapa rekomendasi perbaikan yang dapat dilakukan, yaitu:

1. Memblokir atau menon-aktifkan port TCP 445 jika tidak digunakan. Khususnya memblokir port SMB yang dapat diakses melalui internet. Menonaktifkan port SMB juga memiliki dampak pada operasional seperti tidak bisa melakukan file sharing ataupun printer sharing;
2. Mengikuti panduan Microsoft untuk mengamankan SMB Traffic yang dapat diakses melalui tautan berikut https://docs.microsoft.com/windows-server/storage/file-server/smbsecure-traffic;
3. Melakukan pemeriksaan terhadap versi Sistem Operasi Windows dan Build Number;
4. Melakukan pemutakhiran sistem operasi Windows yang digunakan ke versi terbaru atau menerapkan patch keamanan Microsoft bulan April 2022 atau menerapkan patch lainnya yang relevan;

5. Melakukan deteksi CVE-2022-26809 dengan melakukan pemeriksaan dari port default SMB, RPC client-server communication, dan HTTP RPC Ep Map yang ada di Indonesia dan memiliki layanan Microsoft RPC Endpoint Mapper.

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

Jl. Harsono RM No. 70, Ragunan
Pasar Minggu, Jakarta Selatan, 12550