IMBAUAN KEAMANAN KERENTANAN *REMOTE CODE EXECUTION* (RCE) PADA *WINDOWS RUNTIME* (CVE-2022-21971)

Jumat, 26 Agustus 2022

Ringkasan Eksekutif

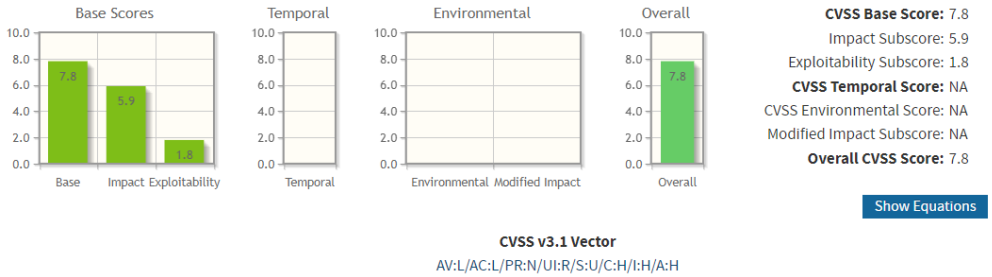
1. Pada tanggal 9 Februari 2022, *National Vulnerability Database* (NVD) NIST merilis kerentanan terhadap *windows runtime.*
2. Kerentanan ini dideskripsikan pada CVE-2022-21971.
3. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

Windows runtime adalah komponen platform dan arsitektur aplikasi pada server sistem operasi *Windows*. Pada tanggal 9 Februari 2022, *National Vulnerability Database* (NVD) NIST merilis kerentanan *Remote Code Execution* (RCE) pada *windows runtime*. Kerentanan ini memungkinkan penyerang melakukan eksekusi kode arbitrer secara jarak jauh pada sistem target. Eksploitasi yang berhasil dapat mengakibatkan suatu sistem menjadi rentan dan terkompromi sepenuhnya.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan **CVE-2022-21971** memiliki nilai **7.8** yang dikategorikan sebagai kerentanan ***HIGH***. Rincian penilaian tersebut terdapat pada Gambar 1.



Gambar 1. *Base Score* untuk Kerentanan CVE-2022-21971 (CVSS:3.1 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

Produk Terdampak

Adapun produk-produk yang rentan terhadap kerentanan CVE-2022-21971 adalah **OS Windows 10, OS Windows 11 dan Windows Server**

Detail dan Dampak Kerentanan

Kerentanan CVE-2022-21971 merupakan kerentanan yang terdapat pada *windows runtime*. dimana kerentanan ini memungkinkan penyerang melakukan eksekusi kode arbitrer secara jarak jauh pada sistem target. Kerentanan ini terdapat pada kesalahan *boundary* saat memproses file dengan ekstensi berkas berupa *Rich Text Format* (RTF) di *windows runtime*. Penyerang jarak jauh dapat membuat dokumen dalam bentuk format *.rtf* secara khusus untuk mengelabui korban agar membukanya sehingga dapat memicu kerusakan memori pada sistem dan melakukan eksekusi kode arbitrer pada sistem target.

Kerentanan ini adalah kerentanan *high*, karena *windows runtime* yang dimaksud rawan terhadap serangan RCE yang berakibat terjadinya sistem yang terkompromi. Berikut rincian kerentanan CVE-2022-21971.

Associated CVE ID	CVE-2022-21971
Description	Kerentanan *Windows Runtime*
Associated ZDI ID	-
CVSS Score	7.8 (High)
Vector	CVSS:3.1/ AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Impact Score	-
Exploitability Score	-
Attack Vector (AV)	Local
Attack Complexity (AC)	Low
Privilege Required (PR)	None
User Interaction (UI)	Required
Scope	Unchanged
Confidentiality (C)	High
Integrity (I)	High
Availability (A)	High

Tabel 1. Rincian Kerentanan CVE-2022-21971

(https[:]//nvd.nist.gov/vuln/detail/CVE-2022-21971)

Panduan Mitigasi

Sebagai langkah pencegahan terhadap kerentanan yang ada, lakukan pembaharuan sistem *patch* keamanan pada OS *Windows* yang dapat dilihat pada [1].

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Jumat, 26 Agustus 2022

Ketentuan Penggunaan Dokumen

Dokumen Imbauan ini tersedia secara bebas dengan mengakses portal Website ID-SIRTII/CC. Terkait penggunaan dokumen imbauan ini, dapat digunakan oleh seluruh pihak yang menggunakan produk terdampak kerawanan yang diulas pada dokumen imbauan ini.

Referensi

[1] "Windows Runtime Remote Code Execution Vulnerability" https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21971 (accessed August 26, 2022).

[2] "Remote Code Execution in Microsoft Windows Runtime" https://www.cybersecurity-help.cz/vdb/SB2022020833 (accessed August 26, 2022).

[3] "Common Vulnerability Scoring System Calculator CVE-2022-219711" https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?name=CVE-2022-21971&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H&version=3.1&source=Microsoft%20Corporation (accessed August 26, 2022).

[4] "Microsoft CVE-2022-21971: Windows Runtime Remote Code Execution Vulnerability" https://www.rapid7.com/db/vulnerabilities/msft-cve-2022-21971/ (accessed August 26, 2022).

[5] "Microsoft Windows Up To Server 2022 Runtime Remote Code Execution" https://vuldb.com/?id.192537 (accessed August 26, 2022).

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

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

DIREKTORAT OPERASI KEAMANAN SIBER
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER