IMBAUAN KEAMANAN KERENTANAN IMPROPER CERTIFICATE VALIDATION PADA LIBREOFFICE (CVE 2022-26305)

Senin, 01 Agustus 2022

Ringkasan Eksekutif

1. Pada 25 Juli 2022 kerentanan *improper certificate validation* pada LibreOffice dirilis.
2. Kerentanan ini dideskripsikan pada CVE 2022-26305 sebagai kerentanan yang memiliki dampak *High* dengan nilai 8.8.
3. Mengingat dampak yang mungkin muncul dari eksploitasi kerentanan ini, diharapkan pengguna dari produk terdampak ataupun pengguna pemerintah dan publik lainnya untuk segera melakukan tindakan-tindakan mitigasi yang dijelaskan pada imbauan keamanan ini.

Pendahuluan

LibreOffice memiliki kerentanan keamanan pada validasi sertifikat yang tidak tepat karena hanya dilakukan dengan membandingkan nomor seri dan *string* penerbit sertifikat yang digunakan dengan sertifikat terpercaya. Kerentanan tersebut pertama kali diidentifikasi pada 28 Februari 2022. Kemudian pada 25 Juli 2022 LibreOffice menerbitkan *patch* untuk memperbaiki *bug* validasi sertifikat yang tidak tepat.

Nilai Kerentanan

Berdasarkan CVSS 3.1, kerentanan ini memiliki nilai **8.8** yang dideskripsikan dengan **CVE 2022-26305** dan dikategorikan sebagai **High.**

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

Gambar 1. *Base Score* untuk Kerentanan CVE-2022-26305
Vector String (CVSS:3.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)

Produk Terdampak

Produk yang terdampak oleh CVE-2022-26305 ditemukan pada produk LibreOffice versi 7.2 sebelum 7.2.7 dan versi 7.3 sebelum 7.3.1.

Detail dan Dampak Kerentanan

LibreOffice mendukung eksekusi makro, yaitu serangkaian perintah yang disimpan untuk digunakan pada suatu waktu. Secara *default*, LibreOffice mengeksekusi makro hanya jika disimpan di lokasi *file* tepercaya atau jika ditandatangani oleh sertifikat tepercaya (*trusted certificate*). Untuk menentukan apakah makro ditandatangani oleh penulis tepercaya (*trusted author*), LibreOffice mencocokkan sertifikat yang digunakan dengan daftar sertifikat tepercaya yang disimpan dalam *database* konfigurasi pengguna.

Kerentanan *improper certificate validation* pada LibreOffice berasal dari *bug* validasi sertifikat yang hanya membandingkan nomor seri dan *string* penerbit sertifikat yang digunakan dengan sertifikat terpercaya. Hal tersebut tidak cukup untuk memverifikasi karena penyerang dapat membuat sertifikat arbitrer dengan nomor seri dan *string* penerbit yang identik dengan sertifikat terpercaya sehingga LibreOffice akan menampilkan sebagai penulis terpercaya. Kemudian penyerang dapat mengarahkan ke pengguna untuk mengeksekusi kode arbitrer yang terdapat dalam makro yang tidak tepat.

Panduan Mitigasi

Untuk melakukan pencegahan terhadap kerentanan CVE-2022-26305, pengguna dapat melakukan pembaruan yang disediakan oleh LibreOffice pada versi >= 7.2.7 dan >= 7.3.2.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Senin, 01 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] “CVE-2022-26305” https://www.libreoffice.org/about-us/security/advisories/cve-2022-26305 (accessed August. 1,2022)

[2] “Improper Certificate Validation” https://security.snyk.io/vuln/SNYK-UNMANAGED-LIBREOFFICE-2960425 (accessed August. 1,2022)

[3] “CVE-2022-26305 Detail” https://www.cve.org/CVERecord?id=CVE-2022-26305 (accessed August. 1,2022)

[4] “LIBREOFFICE UP TO 7.2.6/7.3.0 CERTIFICATE VALIDATION” https://vuldb.com/?id.205037 (accessed August. 1,2022)

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