IMBAUAN KEAMANAN KERENTANAN *ZERO-DAY* PADA GOOGLE CHROME

Jumat, 19 Agustus 2022

Ringkasan Eksekutif

1. Pada bulan Agustus 2022, Google telah mengeluarkan *patch* keamanan terbaru mengenai kerentanan *zero-day* pada *browser* Google Chrome.
2. Kerentanan yang diperbaiki dalam *patch* tersebut didefinisikan pada CVE-2022-2856.
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

Pada tahun 2022 ini, tercatat terdapat empat kerentanan *zero-day* yang telah dilakukan *patching* oleh Google. Pada bulan Februari terdapat kerentanan zero-day pada WebRTC Google Chrome yang didefinisikan dengan CVE-2022-2294. Kemudian pada bulan Maret terdapat kerentanan pada mesin JavaScript Chrome V8 yang memungkinkan penyerang mengeksekusi kode arbitrer (CVE-2022-1096). Lalu pada bulan April dan Juli terdapat kerentanan yang didefinisikan pada CVE-2022-1364 dan CVE-2022-2294. Sampai dengan bulan Agustus 2022, Google telah melakukan *patching* terhadap lima kerentanan *zero-day* yang ditemukan di Chrome. Kerentanan *zero-day* kelima yang baru-baru ini ditemukan yaitu adanya proses validasi input yang tidak memadai, kerentanan ini didefinisikan dalam CVE-2022-2856. Berdasarkan informasi yang dikeluarkan oleh Google, kerentanan ini menjadi target eksploitasi yang sedang marak dilakukan penyerangan saat ini.

Nilai Kerentanan

Level kerentanan CVE-2022-2856 belum didefinisikan.

Produk Terdampak

Produk yang terdampak oleh CVE-2022-2856 ditemukan pada *browser* Google Chrome.

Detail dan Dampak Kerentanan

Berdasarkan informasi yang dikeluarkan oleh Google, kerentanan pada CVE-2022-2856 terjadi pada bagian API *browser* Google Chrome yang memungkinkan *browser* membuka aplikasi luar ketika pengguna mengakses *browser* Google Chrome. Kerentanan ini memiliki potensi berbahaya ketika penyerang melakukan eksploitasi untuk serangan lebih lanjut dengan tingkat yang lebih tinggi. *Bug* yang muncul pada kerentanan ini bermula saat pengguna menggunakan *Intent* untuk tujuan tertentu, jika aktor ancaman dapat membuat respons khusus maka mereka dapat melakukan eksekusi kode pada sistem target.

Intent merupakan sebuah jembatan yang menghubungkan interaksi aktivitas antar komponen aplikasi yang biasanya digunakan pada sistem Android. Pada aplikasi Google Chrome, *Intent* merupakan pengganti *deep linking* untuk skema URI pada perangkat Android dalam *browser* Chrome. Dengan menggunakan fitur *Intent,* penyerang dapat melakukan serangan jarak jauh untuk mengelabui korban dengan membuka halaman *web* yang dibuat khusus sehingga korban mengeksekusi kode arbitrer pada sistem tanpa disadari oleh pengguna itu sendiri. Selain itu, penyerang juga dapat melakukan eksploitasi tambahan sehingga dapat menyebabkan rantai kerentanan baru yang terjadi di kemudian hari.

Panduan Mitigasi

Untuk melakukan pencegahan terhadap kerentanan CVE-2022-2856, perlu dilakukan pembaruan versi Google Chrome dari sisi pengguna maupun administrator ke versi terbaru.

Riwayat Dokumen

Versi Dokumen	Tanggal Rilis
1.0	Kamis, 11 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] "Google Patches Chrome's Fifth ZER-Day of the Year", [Online]. Available: https://threatpost.com/google-patches-chromes-fifth-zero-day-of-the-year/180432/ [Accessed August 19th 2022].

[2] "Google fixes fifth Chrome zero-day bug exploited this year", [Online]. Available: https://www.bleepingcomputer.com/news/security/google-fixes-fifth-chrome-zero-day-bug-exploited-this-year/ [Accessed August 19th 2022].

[3] "New Google Chrome Zero-Day Vulnerability Being Exploited in the Wild", [Online]. Available: https://thehackernews.com/2022/08/new-google-chrome-zero-day.html [Accessed August 19th 2022].

[4] "Update Chrome now! Google issues patch for zero day spotted in the wild", [Online]. Available: https://www.malwarebytes.com/blog/news/2022/08/update-chrome-now-google-issues-patch-for-zero-day-spotted-in-the-wild [Accessed August 19th 2022].

[5] "Google patches yet another Chrome zero-day vulnerability", [Online]. Available: https://www.techtarget.com/searchsecurity/news/252523951/Google-patches-yet-another-Chrome-zero-day-vulnerability [Accessed August 19th 2022].

KONTAK KAMI

(021) 788 33610

bantuan70@bssn.go.id

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