www.idsirtii.or.id

29 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 223

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	1
URGENT	0	1	2
IMPORTANT	1	1	0

General News

AS Melarang Peralatan Telekomunikasi China dan Kamera Pengintai Karena Risiko Keamanan Nasional

Federal Communications Commission (FCC) Amerika Serikat secara resmi mengumumkan tidak akan lagi mengizinkan peralatan elektronik dari Huawei, ZTE, Hytera, Hikvision, dan Dahua, karena dianggap akan menimbulkan ancaman keamanan nasional yang "tidak dapat diterima". Semua perusahaan telekomunikasi dan sistem pengawasan dari China tersebut sebelumnya sudah dimasukkan dalam "*Covered List*" pada 12 Maret 2021. Bukan hanya AS. Inggris, juga melakukan langkah serupa, dengan melarang pemasangan sistem pengawasan visual yang diperoleh dari China di situs pemerintah yang "sensitif". "Departemen telah diberitahu bahwa tidak boleh ada peralatan semacam itu yang dihubungkan ke jaringan inti departemen yang digunakan di lokasi sensitif" kata pemerintah Amerika Serikat.

Prioritas: *3. Important*

< https://thehackernews.com/2022/11/us-bans-chinese-telecom-equipment-and.html >

Breachs/Hacks/Leaks

487 Juta Data WhatsApp Termasuk dari RI Diklaim Bocor, Meta Bantah

Meta membantah berita mengenai bocornya 487 juta data nomor kontak WhatsApp, termasuk didalamnya terdapat 130.331 data dari Indonesia. Meta menyebut tidak menemukan bukti kebocoran data tersebut. Sebelumnya, berita kebocoran data itu diunggah di forum komunitas peretasan terkenal pada 16 November. Juru bicara dari WhatsApp menekankan bahwa perusahaan akan menanggapi berita tentang pelanggaran keamanan layanannya "dengan sangat serius" dan telah mengambil langkah segera untuk menyelidiki lebih lanjut klaim tersebut. Berdasarkan tangkapan layar forum kebocoran data itu yang berjudul "487 million whatsapp users database" terdapat keterangan bahwa data tersebut berasal dari 84 negara, beberapa negaranya adalah Afghanistan sebanyak 558.393 data, Hong Kong 2.937.841 data, Afrika 14.323.766 data, India 6.162.450 data, Indonesia 130.331 data, Rusia 9.996.405 data, Amerika Serikat 32.315.282 data, dan terbesar dari Mesir 44.823.547 data.

Prioritas: *3. Important*

< https://www.cnnindonesia.com/teknologi/20221128063523-192-879545/487-juta-data-whatsapp-termasuk-dari-ri-diklaim-bocor-meta-bantah >

5,4 juta Data Pengguna Twitter Yang Bocor Telah Disebarluaskan

Lebih dari 5,4 juta data pengguna Twitter berisi informasi pribadi yang dicuri menggunakan kerentanan API telah dibagikan secara gratis di forum peretas. Selain data dari Twitter, *dump* data besar-besaran lainnya, yang berpotensi lebih signifikan, juga telah disebarluaskan, hal ini menunjukkan seberapa luas kerentanan pada API dapat disalahgunakan oleh pelaku ancaman. Data yang disebarluaskan tersebut terdiri dari informasi seperti nomor telepon pribadi dan alamat email yang tidak dimaksudkan untuk diketahui secara umum. Data-data tersebut dikumpulkan pada Desember 2021 memanfaatkan celah kerentanan API Twitter yang ditemukan dalam program *bounty bug* dari HackerOne. Celah kerentanan tersebut memungkinkan orang untuk mengambil informasi pribadi dari API.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/?&web_view=true >

Vulnerabilities

Peretas Mengeksploitasi Kerentanan *Remote Code Execution* (RCE) di Windows Internet Key Exchange

Kerentanan RCE kritikal di Ekstensi Protokol Windows Internet Key Exchange (IKE) saat ini aktif dieksploitasi dalam kampanye serangan. Kampanye serangan "*流血你*" yang diterjemahkan menjadi "Bleed You" diduga dioperasikan oleh kelompok kejahatan siber berbahasa Mandarin yang tidak dikenal. Peneliti CYFIRMA telah menemukan lebih dari 1.000 sistem yang terpapar kerentanan ini (CVE-2022-34721). Kerentanan pada kode protokol IKEv1 ini yang berdampak pada OS Windows, Windows Server 2008, Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows 7, Windows 8.1, Windows 10, dan Windows 11. Tujuan akhir dari kampanye serangan ini adalah untuk memfasilitasi serangan malware dan ransomware dan pergerakan lateral di seluruh jaringan. Kampanye ini menargetkan organisasi ritel, konglomerat industri, pemerintah, layanan keuangan, layanan TI, dan industri *e-commerce* di AS, Inggris, Australia, Kanada, Prancis, Jerman, Turki, Jepang, India, UEA, dan Israel.

Prioritas: *2. Urgent*

< https://cyware.com/news/hackers-exploit-rce-vulnerability-in-windows-internet-key-exchange-ce908a01 >

Perbarui Browser Chrome Sekarang untuk Memperbaiki Kerentanan *Zero-Day* Baru yang Aktif Dieksploitasi

Google telah merilis pembaruan untuk mengatasi kerentanan *zero-day* pada di browser web Chrome. Didefinisikan sebagai CVE-2022-4135, kerentanan yang dikategorikan *high* ini merupakan *heap buffer overflow* dalam komponen GPU. Clement Lecigne dari Google's Threat Analysis Group (TAG) adalah orang pertama yang melaporkan kerentanan tersebut pada 22 November 2022. *Bug buffer overflow* berbasis *heap* dapat dipersenjatai oleh pelaku kejahatan siber untuk menghentikan program atau mengeksekusi kode arbitrer, yang mengarah ke perilaku yang tidak diinginkan. Pengguna disarankan untuk memperbarui ke versi 107.0.5304.121 untuk macOS dan Linux dan 107.0.5304.121/.122 untuk Windows untuk mengurangi potensi ancaman. Pengguna browser berbasis Chromium seperti Microsoft Edge, Brave, Opera, dan Vivaldi juga disarankan untuk menerapkan perbaikan saat tersedia.

Prioritas: *1. Critical*

< https://thehackernews.com/2022/11/update-chrome-browser-now-to-patch-new.html >

Perangkat Dell, HP, dan Lenovo Ditemukan Menggunakan Versi OpenSSL yang Kedaluwarsa

Analisis *firmware* di seluruh perangkat dari Dell, HP, dan Lenovo ditemukan bahwa terdapat versi usang dari OpenSSL pada CryptoPkg, hal ini dapat berisiko munculnya *supply chain attack*. Dari hasil analisis perusahaan keamanan *firmware* Binarly, *firmware* perangkat Lenovo Thinkpad ditemukan menggunakan tiga versi berbeda dari OpenSSL: 0.9.8zb, 1.0.0a, dan 1.0.2j, yang dirilis pada 2018. Beberapa paket firmware dari Lenovo dan Dell menggunakan versi yang lebih lama (0.9.8l), yang keluar pada tanggal 5 November 2009. Kode firmware HP juga menggunakan versi OpenSSL yang dirilis 10 tahun yang lalu (0.9.8w).

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/dell-hp-and-lenovo-devices-found-using.html >