www.idsirtii.or.id

17 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 215

OVERVIEW

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

General News

Jokowi: Kebocoran Data Bisa Bikin Rugi USD 5 Triliun

Dalam sesi ketiga KTTG20 Bali yang mengusung tema *Digital Transformation*, Jokowi menekankan pentingnya membangun dunia digital yang aman untuk semua penduduk dunia. Jokowi mengatakan saat ini ekonomi digital sudah menjadi salah satu kontributor besar dalam pendapatan domestik bruto (PDB) global dan ia mengajak pemimpin dunia untuk mendukung percepatan transformasi digital. Jokowi membeberkan tiga masalah yang harus menjadi fokus untuk mempercepat transformasi digital. Pertama, akses internet yang masih tidak merata. Kedua, transformasi digital harus didukung dengan literasi digital. Ketiga, membangun dunia digital yang aman. Menurut Jokowi, saat ini lingkungan digital masih dipenuhi dengan *hoax* dan perundungan siber yang bisa memecah persatuan. Belum lagi kasus kebocoran data akibat kejahatan siber yang disebut Jokowi bisa menimbulkan kerugian hingga USD 5 triliun pada tahun 2024.

Prioritas: *3. Important*

< https://www.latimes.com/business/technology/story/2022-11-11/ransomware-gangs-shift-tactics-making-crimes-harder-to-track?&web_view=true >

Breachs/Hacks/Leaks

Peneliti Temukan Ratusan Amazon RDS *Instances* yang Membocorkan Data Pribadi Pengguna

Ratusan *database* di Amazon Relational Database Service bocor dan mengungkap *Personal Identifiable Information* termasuk nama, alamat *email,* nomor telepon, tanggal lahir, status perkawinan, dan beberapa informasi lainnya. Berdasarkan sifat informasi yang diungkap, *threat actor* mencuri data untuk keuntungan finansial atau memanfaatkannya untuk lebih memahami lingkungan TI perusahaan, yang kemudian dapat bertindak sebagai batu loncatan untuk upaya pengumpulan informasi rahasia. Sangat disarankan agar *snapshot* RDS tidak dapat diakses publik untuk mencegah potensi kebocoran atau penyalahgunaan data sensitif. Juga disarankan untuk mengenkripsi *snapshot* jika memungkinkan.

Prioritas: *2. Urgent*

< https://www.bleepingcomputer.com/news/security/whoosh-confirms-data-breach-after-hackers-sell-72m-user-records/?&web_view=true >

Bjorka Ambil 3,2 Miliar Data PeduliLindungi, Pengamat: Ini Pertanyaan Besar

Hacker Bjorka kembali menjalankan aksinya, kali ini dia membobol data dari PeduliLindungi. Padahal, sekitar seminggu sebelumnya, ia mengaku berhasil mengambil data MyPertamina. Terlihat Bjorka mempublikasikan pada tanggal 15 November 2022, dengan judul 3,2 miliar data Covid-19 di Indonesia dari aplikasi PeduliLindungi. Pengamat keamanan siber dari Vaksincom, Alfons Tanujaya, menduga data tersebut kemungkinan besar valid. Namun, ia heran karena Bjorka sanggup menjebol pertahanan pengamanan. Menurutnya, jika memang menerapkan ISO 27001 dengan baik, bisa dilakukan mitigasi. Ia meminta pihak yang bertanggung jawab tidak diam saja. Sekilas terlihat data PeduliLindungi yang ditawarkan Bjorka adalah data terkompres sebesar 48 GB dan tidak dikompres sebesar 157 GB dengan total 3.250.144.777 data.

Prioritas: *1. Critical*

< https://tekno.tempo.co/read/1657704/top-3-tekno-berita-hari-ini-analisis-kebugaran-berbasis-big-data-diplomasi-mangrove >

Vulnerabilities

Kampanye RapperBot Baru Meluncurkan Serangan DDoS di Server Game

Peneliti keamanan siber telah menemukan sampel *malware* baru yang disebut dengan RapperBot. *Malware* ini digunakan untuk membangun *botnet* yang mampu meluncurkan serangan *Distributed Denial of Service* (DDoS) terhadap server *game.* RapperBot pertama kali didokumentasikan oleh perusahaan keamanan jaringan pada Agustus 2022. Versi RapperBot yang baru memiliki kemampuan untuk melakukan *Telnet brute-force*, mendukung serangan DoS menggunakan protokol *tunneling Generic Routing Encapsulation* (GRE) serta UDP *flood* yang menargetkan server game yang menjalankan Grand Theft Auto: San Andreas.

Prioritas: *2. Urgent*
< https://thehackernews.com/2022/11/warning-new-rapperbot-campaign-aims-to.html?&web_view=true >

PCspooF: Kerentanan Baru Mempengaruhi Teknologi Jaringan yang Digunakan oleh Pesawat Luar Angkasa dan Pesawat Terbang

Sebuah kerentanan baru dari teknologi yang disebut *time-triggered ethernet* (TTE) telah ditemukan. Teknologi tersebut digunakan dalam infrastruktur keselamatan penting yang berpotensi menyebabkan kegagalan sistem dalam menggerakkan pesawat ruang angkasa dan pesawat terbang. Dijuluki PCspooF oleh sekelompok akademisi dan peneliti dari University of Michigan, University of Pennsylvania, dan NASA Johnson Space Center, teknik ini dirancang untuk mematahkan jaminan keamanan TTE dan menyebabkan perangkat TTE kehilangan sinkronisasi hingga satu detik. Hal ini dapat menyebabkan manuver yang tidak terkendali dalam misi penerbangan luar angkasa dan mengancam keselamatan awak.

Prioritas: *1. Critical*
< https://thehackernews.com/2022/11/pcspoof-new-vulnerability-affects.html?&web_view=true >

Firefox 107 Menambal Kerentanan Tinggi

Mozilla telah mengumumkan perilisan Firefox 107 yang menambal sejumlah besar kerentanan. Sebanyak 19 CVE telah diperbaiki oleh Firefox 107. Sembilan di antaranya merupakan kerentanan dengan *high severity* yang dapat menyebabkan pengungkapan informasi, *spoofing*, dan crash atau eksekusi kode arbitrer akibat *bug*

use-after-free. Beberapa kerentanan dengan *medium severity* sedang juga dapat menyebabkan *bypass* keamanan dan serangan spoofing. Masalah berdampak rendah yang ditambal di Firefox terkait dengan *security exception* dan *spoofing*. Firefox memang tidak sepopuler Chrome, namun Firefox *tetap* menjadi target yang menggiurkan.

Prioritas: *2. Urgent*

< https://www.securityweek.com/firefox-107-patches-high-impact-vulnerabilities?&web_view=true >