CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 219

23 November 2022

OVERVIEW

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

General News

Microsoft Memperingatkan *Remote Desktop* mengalami *Freeze* pada Windows 11 22H2

Microsoft sedang menyelidiki dan berupaya memperbaiki masalah *Remote Desktop* pada sistem Windows 11 setelah menginstal Pembaruan Windows 11 2022. Setelah menginstal Windows 11, versi 22H2 (juga disebut Pembaruan Windows 11 2022), aplikasi Windows Remote Desktop mungkin berhenti merespons saat terhubung melalui *gateway* Remote Desktop atau Broker Koneksi Desktop Jarak Jauh. Contoh skenario koneksi ini adalah saat menghubungkan ke koleksi Layanan Desktop Jarak Jauh. RemoteApp dan Desktop Connections. Pengguna rumahan kemungkinan tidak akan mengalami masalah saat menggunakan aplikasi karena menggunakan proses koneksi yang berbeda dari yang ada di perangkat perusahaan, yang terpengaruh oleh masalah umum ini. Saat ini sedang dikerjakan resolusi, dengan detail lebih lanjut mengenai masalah ini akan diberikan dalam pembaruan mendatang.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/microsoft/microsoft-warns-of-remote-desktop-freezes-on-windows-11-22h2/ >

Menkominfo Sebut KPU Harus Serius Perhatikan Pertahanan Serangan Siber dan Menyinggung Tentang "*Penetration Test*"

Menkominfo, Johnny G Plate menekankan bahwa KPU RI harus memerhatikan betul kemampuan bertahan dari serangan siber jelang Pemilu 2024. Terlebih, berdasarkan Undang-Undang Pelindungan Data Pribadi (PDP), kini KPU termasuk sebagai salah satu PSE yang memiliki tanggung jawab besar dalam pelindungan data pribadi. Tangguh atau tidaknya sistem elektronik KPU jadi pertaruhan karena bakal menentukan legitimasi Pemilu 2024, terlepas dari segala kerja keras dan desain pemilu yang dikerjakan oleh KPU RI untuk menyukseskan Pemilu 2024. Johnny G Plate bahkan menyinggung jajarannya untuk memberikan bantuan kerja sama melakukan *penetration test* atau uji penetrasi terhadap sistem elektronik KPU RI. Uji penetrasi merupakan sejenis simulasi serangan siber atau peretasan secara etik guna menguji ketangguhan sebuah sistem menghadapi peretasan atau pembobolan.

Prioritas: ***2. Urgent***

< https://nasional.kompas.com/read/2022/11/22/15524031/menkominfo-sebut-kpu-harus-serius-perhatikan-pertahanan-serangan-siber >

Breachs/Hacks/Leaks

Dua Warga Estonia Ditangkap Dalam Skema Penipuan Mata Uang Kripto Senilai $575 Juta

Dua warga negara Estonia ditangkap di Tallinn, Estonia, setelah didakwa di AS karena menjalankan skema Ponzi *cryptocurrency* penipuan yang menyebabkan kerugian lebih dari $575 juta. Menurut surat dakwaan, Sergei Potapenko dan Ivan Turõgin, keduanya berusia 37 tahun, diduga menipu ratusan ribu korban melalui skema *crypto* Ponzi. Duo ini menggunakan *shell companies* untuk mencuci uang tunai dari aktivitas penipuan dan membeli real estat serta mobil mewah. Mereka membujuk para korban untuk masuk ke dalam kontrak persewaan peralatan penipuan dengan layanan penambangan *cryptocurrency* milik terdakwa yang disebut HashFlare. Mereka juga menyebabkan korban berinvestasi di bank mata uang virtual bernama Polybius Bank. Para terdakwa dituduh telah menipu para korban antara Desember 2013 dan Agustus 2019, mereka beroperasi dengan rekan konspirator lainnya yang tinggal di Estonia, Belarusia, dan Swiss.

Prioritas: ***3. Important***

< https://securityaffairs.co/wordpress/138823/cyber-crime/estonian-575m-cryptocurrency-fraud-scheme.html >

Vulnerabilities

Aplikasi Pengelola *File* Android Menginfeksi Ribuan Orang dengan *Malware* Sharkbot

Kumpulan baru aplikasi Android berbahaya yang berpura-pura sebagai pengelola *file* yang tidak berbahaya telah menyusup ke market aplikasi resmi Google Play, menginfeksi pengguna dengan trojan perbankan Sharkbot. Aplikasi tidak membawa muatan berbahaya saat penginstalan untuk menghindari deteksi saat dikirimkan di Google Play, tetapi mengambil muatannya nanti dari sumber jarak jauh. Karena aplikasi trojan adalah pengelola *file*, kecil kemungkinannya menimbulkan kecurigaan saat meminta izin berbahaya untuk memuat *malware* Sharkbot.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/security/android-file-manager-apps-infect-thousands-with-sharkbot-malware/ >

Kerentanan Firmware BMC Mengekspos OT, Perangkat IoT Terhadap Serangan Jarak Jauh

BMC adalah prosesor khusus yang memungkinkan administrator mengontrol dan memantau perangkat dari jarak jauh tanpa harus mengakses sistem operasi atau aplikasi yang berjalan di dalamnya. Banyak kerentanan BMC telah ditemukan dalam beberapa tahun terakhir, dengan para peneliti memperingatkan bahwa eksploitasi kelemahan ini dapat memungkinkan penyerang merusak server yang ditargetkan. Riset Nozomi Networks menargetkan BMC yang digunakan untuk teknologi operasional (OT) dan perangkat IoT. Nozomi telah menganalisis IAC-AST2500A, sebuah kartu ekspansi yang memungkinkan fungsionalitas BMC pada peralatan jaringan. *Firmware* yang berjalan pada kartu yang terpengaruh didasarkan pada *firmware* manajemen jarak jauh BMC dari AMI, yang digunakan oleh perusahaan teknologi seperti Asus, Dell, HP, Lenovo, Gigabyte, dan Nvidia.

Prioritas: ***3. Important***

<https://www.securityweek.com/bmc-firmware-vulnerabilities-expose-ot-iot-devices-remote-attacks?&web_view=true >

5 Kerentanan API yang Dieksploitasi oleh Penjahat

Bukan rahasia lagi bahwa keamanan dunia maya telah menjadi prioritas utama bagi sebagian besar organisasi terutama di industri yang menangani informasi pelanggan yang sensitif. Karena bisnis ini berupaya membangun strategi keamanan yang kuat, sangat penting bagi mereka untuk memperhitungkan berbagai vektor ancaman dan kerentanan. Salah satu area yang memerlukan pengawasan signifikan adalah keamanan API. API, kependekan dari *Application Programming Interface*, telah menjadi blok bangunan umum untuk organisasi yang diaktifkan secara digital. API memfasilitasi komunikasi serta operasi bisnis penting dan juga mendukung transformasi digital yang penting. Maka tidak mengherankan jika rata-rata jumlah API per perusahaan meningkat 221% pada tahun lalu. Dalam 10 Teratas Keamanan API, Proyek Keamanan Aplikasi Web Terbuka (OWASP) mengidentifikasi sepuluh ancaman teratas terhadap API. Lima kerentanan API yang paling umum dieksploitasi oleh penyerang diantaranya yaitu *Broken Object Level Authentication* (BOLA), *Broken User Authentication*, *Excessive Data Exposure*, *Lack of Resources and Rate Limiting*, dan *Security Misconfiguration*.

Prioritas: ***2. Urgent***

< https://securityaffairs.co/wordpress/138879/security/5-api-vulnerabilities.html >