www.idsirtii.or.id

13 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 103

OVERVIEW

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

General News

Peretas Iran Menggunakan DNS *Hijacking Malware* dalam Serangan Terbaru

Aktor ancaman yang disponsori oleh Negara Iran telah beralih menggunakan *backdoor* berbasis .NET dalam kampanye yang baru-baru ini dilakukan terhadap Timur Tengah. *Malware* ini memanfaatkan teknik serangan DNS yang disebut 'DNS *Hijacking*' di mana server DNS yang dikendalikan penyerang memanipulasi respons permintaan DNS dan menyelesaikannya sesuai kebutuhan jahat mereka. DNS *Hijacking* adalah serangan pengalihan di mana permintaan DNS ke situs web asli dicegat untuk membawa pengguna ke halaman penipuan yang dikendalikan oleh actor ancaman. DNS *Hijacking* menargetkan DNS *records* pada situs web. Selain menyalahgunakan protokol DNS untuk komunikasi *command-and-control* (C2) guna menghindari deteksi, *malware* tersebut juga mengunggah dan mengunduh file arbitrer ke dan dari server jarak jauh serta menjalankan perintah sistem berbahaya secara *remote* pada host yang disusupi.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/06/iranian-hackers-spotted-using-new-dns.html >

Package PyPI Mengandung *Password Stealer*

Paket PyPI berupa 'keep', 'pyanxdns', 'api-res-py' ditemukan mengandung *backdoor* karena adanya ketergantungan 'request' berbahaya dalam beberapa versi. CVE-2022-30877 – 'keep' versi 1.2, CVE-2022-30882 – 'pyanxdns', dan CVE-2022-31313 – 'api-res-py' versi 0.1 telah ditetapkan berhubungan dengan beberapa versi yang rentan. *Info-Stealing Trojan* yang disisipkan akan mencoba mencuri nama dan kata sandi yang disimpan di *browser web*. Setelah mendapatkan akses terhadap kredensial pengguna, pelaku ancaman kemudian melakukan serangan lebih lanjut.

Prioritas: *1. Critical*

< https://www.bleepingcomputer.com/news/security/pypi-package-keep-mistakenly-included-a-password-stealer/ >

Jalur Eksploitasi Umum yang Dibiarkan Terbuka Bagi Penyerang pada Kuartal Pertama Tahun 2022

Paket Exposed version control repositories, leaked secrets in public code repositories, a subdomain vulnerable to takover, exposed Amazon S3 buckets, dan Microsoft Exchange Server servers vulnerable to CVE-2021-42321 exploitation adalah jalur eksploitasi paling umum dari perusahaan menengah hingga besar yang dibiarkan terbuka untuk penyerang pada Q1 2022, menurut Mandiant. Perusahaan telah mendasarkan daftar pada masalah paling umum yang ditemukan dengan terus memindai permukaan serangan eksternal pelanggannya dari 1 Januari 2022 hingga 31 Maret 2022. Masalah potensial lainnya yang jarang ditemui termasuk layanan dan *port* yang terbuka, konfigurasi ms, dan kerentanan spesifik (mis., di SAP, Log4j, dll.). Eksposur tersebut terjadi terutama karena kurangnya patching yang tepat waktu dan penyimpangan konfigurasi terus-menerus dalam aset yang terhubung ke internet. Kesalahan konfigurasi dan implementasi kebijakan yang buruk juga merupakan alasan utama di balik penyimpanan data yang terbuka.

Prioritas: *3. Important*

< https://www.helpnetsecurity.com/2022/06/09/exploit-paths-enterprises/ >

Vulnerabilities

Botnet Baru Menargetkan Kerentanan Kritis di Server Confluence

Beberapa botnet menyalahgunakan kerentanan RCE kritis untuk menginfeksi server Linux yang menjalankan Atlassian Confluence Server dan Data Center. Eksploitasi kerentanan (CVE-2021-26084) di Server dan Pusat Data Confluence memungkinkan penyerang yang tidak sah untuk membuat akun admin baru, menjalankan perintah, dan mengambil alih server dari jarak jauh. Botnet Kinsing, Hezb, dan Dark.IoT telah

diidentifikasi menargetkan server Linux yang terbuka untuk mengirimkan *backdoors* dan *cryptominers*. Botnet masih menyalahgunakan kelemahan kritis di Confluence Server dan Pusat Data yang belum ditambal. Oleh karena itu, admin disarankan untuk memperbarui server mereka sesegera mungkin untuk menghindari infeksi. Selain itu, Atlassian menyarankan untuk meningkatkan ke versi tetap dari Confluence agar tetap terlindungi.

Prioritas: *2. Urgent*

< https://cyware.com/news/new-botnets-target-critical-vulnerability-in-confluence-servers-9b210f41 >

Patch Pembaruan Chrome 102 Memperbaiki Kerentanan Tingkat Tinggi

Google minggu ini mengumumkan rilis pembaruan *browser* Chrome yang memperbaiki tujuh kerentanan, termasuk empat masalah yang dilaporkan oleh peneliti eksternal. Dilacak sebagai CVE-2022-2007, *bug* pertama ini digambarkan sebagai penggunaan setelah bebas di WebGPU. Celah keamanan dilaporkan oleh David Manouchehri, yang menerima hadiah hadiah bug $10.000 untuk temuannya. Kerentanan use-after-free lainnya yang diatasi dengan pembaruan Chrome ini adalah CVE-2022-2011, kerentanan yang diidentifikasi di ANGLE, lapisan abstraksi mesin grafis Chrome. Bug tersebut dilaporkan oleh SeongHwan Park. Pembaruan Chrome terbaru juga menyelesaikan CVE-2022-2008, akses memori di luar batas di WebGL, yang dilaporkan oleh peneliti Cybersecurity VinCSS Tran Van Khang. Kerentanan keempat yang dilaporkan adalah CVE-2022-2010, merupakan proses pembacaan di luar batas, yang dilaporkan oleh Mark Brand dari Google Project Zero.

Prioritas: *1. Critical*

< https://www.securityweek.com/chrome-102-update-patches-high-severity-vulnerabilities >

PACMAN, Teknik Serangan Baru Terhadap CPU Apple M1

PACMAN adalah teknik serangan perangkat keras baru yang memungkinkan penyerang melewati *Pointer Authentication* (PAC) pada CPU Apple M1. *Pointer Authentication Code* (PAC) memungkinkan untuk mendeteksi dan menjaga terhadap perubahan tak terduga pada *pointer* di memori. Otentikasi *pointer* mengimplementasikan instruksi CPU khusus untuk menambahkan tanda tangan kriptografi (PAC) ke bit orde tinggi *pointer* yang tidak digunakan. Tanda tangan dihapus dan diautentikasi oleh instruksi lain setelah membaca *pointer* kembali dari memori. Setiap perubahan pada nilai yang disimpan antara penulisan dan pembacaan akan membatalkan tanda tangan, hal tersebut ditafsirkan sebagai kerusakan memori dan

menetapkan bit orde tinggi dalam *pointer* untuk membatalkan pointer. Para peneliti yang merancang teknik serangan berspekulasi bahwa prinsip-prinsip di balik serangan PACMAN dapat digunakan untuk lebih dari sekadar PAC.

Prioritas: *1. Critical*

< https://securityaffairs.co/wordpress/132154/hacking/pacman-attack-apple-m1-cpus.html >