'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 227 | 11 DESEMBER 2024

OVERVIEW	Critical	Urgent	Important
General News	0	0	1
Breachs/Hacks/Leaks	0	2	0
Vulnerabilities	0	2	0
Malwares	0	1	0

General News

Wyden Usulkan RUU untuk Mengamankan Telekomunikasi AS Pasca Serangan Salt Typhoon

Senator Ron Wyden mengajukan RUU baru bernama "Secure American Communications Act" untuk memperkuat keamanan jaringan perusahaan telekomunikasi Amerika yang diretas oleh kelompok peretas Salt Typhoon yang didukung negara China. RUU ini menginstruksikan FCC untuk memberlakukan aturan keamanan siber wajib dan mewajibkan penyedia telekomunikasi menguji kerentanan jaringan mereka setiap tahun, menambalnya, serta mendokumentasikan hasil dan langkah perbaikan. Perusahaan juga harus menyewa auditor independen untuk memeriksa kepatuhan terhadap aturan FCC secara tahunan. Wyden menyalahkan kurangnya aturan keamanan yang ketat sebelumnya sebagai penyebab akses peretas terhadap data komunikasi warga AS, termasuk panggilan dan pesan penting. Menanggapi serangan ini, FCC berkomitmen untuk segera mengamanatkan regulasi keamanan baru bagi penyedia layanan telekomunikasi. Serangan Salt Typhoon yang terungkap Oktober lalu mengonfirmasi bahwa peretas China telah mengakses jaringan sejumlah operator AS seperti T-Mobile dan AT&T selama berbulan-bulan. Pemerintah AS menyarankan penggunaan aplikasi pesan terenkripsi untuk mengurangi risiko penyadapan dan mengeluarkan panduan untuk melindungi sistem infrastruktur telekomunikasi dari serangan serupa di masa depan.

Prioritas : 3. Important
Sumber : https://www.bleepingcomputer.com/news/security/wyden-proposes-bill-to-secure-us-telecoms-after-salt-typhoon-hacks/

Breachs/Hacks/Leaks

Peretas Nemesis dan ShinyHunters Bobol 2 TB Data Sensitif melalui Konfigurasi AWS yang Salah

Kelompok peretas Nemesis dan ShinyHunters terlibat dalam operasi siber besar yang mengeksploitasi kerentanan pada situs web publik dengan konfigurasi yang salah, mengakibatkan kebocoran lebih dari 2 TB data sensitif, termasuk informasi pelanggan, kredensial, dan kode sumber. Serangan ini dimulai dengan pemindaian rentang IP AWS menggunakan alat seperti Shodan untuk mengidentifikasi endpoint rentan dan memperluas target melalui analisis sertifikat SSL. Setelah menemukan kelemahan, mereka mengeksploitasi endpoint tersebut untuk mencuri data seperti API keys, kredensial database, dan akses platform seperti GitHub dan Twilio, yang kemudian dijual di pasar gelap dengan harga ratusan euro. Operasi ini memiliki keterkaitan dengan Sebastien Raoult dari grup ShinyHunters yang kini tidak aktif serta Nemesis Blackmarket, yang dikenal menjual data curian. AWS menjelaskan bahwa kebocoran terjadi akibat kesalahan konfigurasi pelanggan, sesuai model tanggung jawab bersama, dan merekomendasikan langkah mitigasi seperti rotasi kunci, penggunaan AWS Secrets Manager, serta penerapan Web Application Firewall (WAF). Meski AWS telah berusaha mengurangi dampak serangan, para ahli menilai bahwa ancaman semacam ini akan terus berlanjut, sehingga pelanggan perlu melakukan penilaian kerentanan secara berkala. Langkah-langkah ini penting untuk melindungi aset digital dan mencegah kebocoran data di masa mendatang.

Prioritas : 2. Urgent
Sumber : https://www.infosecurity-magazine.com/news/hackers-exploit-aws/

Peretas Manfaatkan Visual Studio Code Remote Tunnels untuk Spionase Siber

Sebuah kelompok peretas yang diduga berhubungan dengan China melancarkan serangan terhadap penyedia layanan TI B2B di Eropa Selatan melalui kampanye bernama Operation Digital Eye. Peneliti keamanan dari SentinelOne dan Tinexta Cyber menemukan serangan ini terjadi antara Juni hingga Juli 2024, tetapi berhasil dihentikan sebelum data berhasil dicuri. Kelompok peretas memanfaatkan fitur Visual Studio Code Remote Tunnels dan infrastruktur Microsoft Azure untuk kegiatan command-and-control (C2) yang menyamar sebagai aktivitas sah. Serangan dimulai dengan injeksi SQL menggunakan SQLmap untuk mengakses aplikasi berbasis internet, diikuti dengan pemasangan web shell PHPsert untuk akses jarak jauh. Teknik seperti pass-the-hash dengan alat Mimikatz versi modifikasi juga digunakan untuk menyusup ke sistem lain. Investigasi mengungkapkan kesamaan kode alat peretas ini dengan operasi spionase lain asal China, seperti Operation Soft Cell. Fitur seperti komentar berbahasa Mandarin sederhana di PHPsert dan aktivitas kerja sesuai zona waktu China semakin menguatkan keterlibatan kelompok ini.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2024/12/hackers-weaponize-visual-studio-code.html

Vulnerabilities

Eksploitasi Kerentanan Keamanan Cleo File Transfer, Pengguna Diminta Segera Mitigasi

Kerentanan keamanan pada perangkat lunak transfer file Cleo telah dieksploitasi secara luas sejak 3 Desember 2024, meskipun sistem telah sepenuhnya diperbarui. Kerentanan ini, yang diidentifikasi sebagai CVE-2024-50623, memungkinkan eksekusi kode jarak jauh tanpa otentikasi akibat fitur unggah file yang tidak terbatas. Beberapa produk yang terdampak, seperti Cleo Harmony, VLTrader, dan LexiCom hingga versi 5.8.0.23, saat ini tengah menunggu pembaruan keamanan baru. Peneliti keamanan menemukan bahwa aktor ancaman menggunakan kerentanan ini untuk mengunggah file berbahaya yang memicu perintah PowerShell, mengunduh file Java Archive (JAR) dari server jarak jauh, dan mengenkripsi file dengan ekstensi .termite menggunakan ransomware Termite. Setidaknya 10 organisasi dari sektor logistik, produk konsumen, dan pangan telah menjadi korban, termasuk perusahaan rantai pasokan Blue Yonder. Peneliti juga mencatat bahwa kelompok ransomware Termite, yang mungkin penerus Cl0p, semakin aktif menyerang perangkat lunak transfer file terkelola. Pengguna diimbau memastikan perangkat lunak tidak terpapar internet dan segera memperbarui sistem untuk meminimalkan risiko eksploitasi lebih lanjut.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2024/12/cleo-file-transfer-vulnerability-under.html

Waspada Eksploitasi Zero-Day Windows Common Log File System (CVE-2024-49138), Patch Tersedia!

Kerentanan keamanan serius CVE-2024-49138 ditemukan pada Windows Common Log File System (CLFS) Driver, memungkinkan eskalasi hak istimewa hingga level SYSTEM tanpa interaksi pengguna. Dengan skor CVSS 7.8, Microsoft telah merilis patch melalui pembaruan Patch Tuesday Desember 2024. Kerentanan ini berasal dari buffer overflow berbasis heap yang dapat dieksploitasi oleh aktor ancaman dengan hak akses lokal, memengaruhi kerahasiaan, integritas, dan ketersediaan sistem secara signifikan. CrowdStrike Advanced Research Team melaporkan temuan ini, menggarisbawahi pentingnya kolaborasi keamanan. Sebagai respons, CISA menambahkan kerentanan ini ke dalam Katalog Kerentanan yang Dieksploitasi. Microsoft menyarankan pengguna segera memasang pembaruan keamanan terbaru, memeriksa konfigurasi sistem, dan memantau indikator kompromi untuk mencegah eskalasi. Mengingat kompleksitas serangan yang rendah, kerentanan ini dapat menargetkan berbagai perangkat, sehingga sistem tanpa patch menjadi sangat rentan. Tindakan cepat akan mengurangi risiko kerusakan akibat kerentanan ini.

Prioritas : 2. Urgent
Sumber : https://cybersecuritynews.com/windows-common-log-file-system-zero-day/

Malware

Malware Meeten Baru Targetkan Pengguna macOS dan Windows untuk Curi Kredensial Login

Malware baru bernama Meeten ditemukan menyasar pengguna macOS dan Windows yang menyamar sebagai aplikasi konferensi video palsu. Malware ini dikenal sebagai Realst, telah aktif selama empat bulan terakhir dan menggunakan nama perusahaan palsu seperti "Meetio," "Clusee," "Cuesee," dan "Meetone." Penyerang menggunakan konten yang dihasilkan AI untuk membuat situs web dan profil media sosial yang meyakinkan, lalu memancing korban mengunduh aplikasi yang sebenarnya merupakan pencuri informasi. Dalam beberapa kasus, target menerima pesan Telegram dari akun yang berpura-pura menjadi teman atau kolega untuk mengatur pertemuan bisnis. Selain mencuri kredensial login, malware ini juga mengambil data sensitif seperti informasi kartu bank, kredensial browser, dan dompet cryptocurrency dari Ledger, Trezor, hingga Binance. Versi Windows dari malware ini menggunakan file Rust berbasis binary untuk mengekstraksi data, sementara versi macOS serupa dengan tambahan script JavaScript untuk mencuri cryptocurrency langsung dari browser. Pengguna diimbau waspada terhadap undangan bisnis melalui Telegram dan memverifikasi sumber aplikasi sebelum mengunduh.

Prioritas : 2. Urgent
Sumber : https://cybersecuritynews.com/meeten-ai-malware-attacking-macos-windows/

Ditandatangani secara elektronik oleh:
DIREKTUR OPERASI KEAMANAN SIBER

Andi Yusuf, M.T.
Pembina Utama Muda (IV/c)

KONTAK KAMI

DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

@Id_SIRTII (+62) 811 1065 2018 bantuan70@bssn.go.id