'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 237 | 27 DESEMBER 2024

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

General News

Pencurian Bitcoin senilai $308 juta terkait dengan Korea Utara

Pihak berwenang Jepang dan AS menghubungkan peretasan senilai $308 juta terhadap DMM Bitcoin dengan kelompok Korea Utara, termasuk Lazarus Group. Peretasan ini dilakukan pada Mei 2024 melalui teknik *social engineering* yang menyusup ke sistem Ginco menggunakan skrip Python berbahaya, memungkinkan manipulasi transaksi dan pencurian 4,502.9 BTC. Dana tersebut kemudian ditransfer ke dompet yang dikendalikan penyerang, dengan sebagian tersimpan di dompet yang sebelumnya diidentifikasi FBI. Lazarus Group diketahui terlibat dalam berbagai pencurian *cryptocurrency* besar, termasuk $100 juta dari Atomic Wallet dan $60 juta dari Alphapo pada 2023. FBI memperingatkan perusahaan untuk memeriksa transaksi yang terkait dengan dompet berisiko dan terus memerangi aktivitas ilegal Korea Utara untuk mendanai rezim mereka.

Prioritas : 3. Important
Sumber : https://securityaffairs.com/172290/hacking/dmm-bitcoin-308m-theft-linked-north-korea.html

Breachs/Hacks/Leaks

Japan Airlines Mengalami Serangan Siber yang Berdampak pada Penjualan Tiket

Japan Airlines (JAL) mengalami serangan siber pada Kamis pagi, menyebabkan penangguhan penjualan tiket untuk penerbangan hari itu. Serangan yang dimulai pukul 7:24 pagi ini merupakan serangan *distributed denial-of-service* (DDoS) yang menyebabkan gangguan pada sistem internal dan eksternal JAL, termasuk *router*, tetapi tidak menginfeksi sistem dengan *malware* atau membocorkan data pelanggan. Serangan ini menyebabkan keterlambatan lebih dari 30 menit pada 24 penerbangan

domestik, meskipun sistem JAL kini telah sepenuhnya pulih. Maskapai lain di Jepang, seperti ANA Holdings, Skymark Airlines, dan Star Flyer, tidak terkena dampak serangan ini. Pemerintah Jepang melalui Menteri Transportasi meminta JAL segera memperbaiki sistemnya untuk mengatasi dampak terhadap pelanggan, sementara gangguan pada penerbangan JAL juga berdampak pada pengiriman pos dan parsel oleh Japan Post Co.

Prioritas : 3. Important
Sumber : https://securityaffairs.com/172319/hacking/japan-airlines-hit-cyberattack.html

Vulnerabilities

Kerentanan Platform *Cloud* Ruijie Networks Berdampak pada 50.000 Perangkat Terkena Serangan Jarak Jauh

Peneliti keamanan menemukan beberapa kerentanan serius pada platform manajemen *cloud* Ruijie Networks, termasuk Reyee OS yang memungkinkan penyerang mengambil alih perangkat jaringan dan mengontrol puluhan ribu perangkat yang terhubung ke *cloud*. Tiga kerentanan kritis, seperti mekanisme pemulihan kata sandi yang lemah (CVE-2024-47547), *server-side request forgery* (CVE-2024-48874), dan eksekusi perintah OS melalui pesan MQTT (CVE-2024-52324), dapat dimanfaatkan untuk eksekusi kode jarak jauh. Serangan "Open Sesame" memungkinkan akses ilegal ke perangkat hanya dengan mengetahui nomor seri perangkat. Meskipun semua kerentanan ini telah diperbaiki oleh Ruijie, sekitar 50.000 perangkat sempat terdampak. Selain itu, PCAutomotive menemukan 12 kerentanan pada unit infotainment MIB3 Skoda yang memungkinkan pelacakan lokasi, perekaman suara, dan pencurian data sensitif.

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2024/12/ruijie-networks-cloud-platform-flaws.html

Kerentanan *SQL Injection* Kritis di Apache Traffic Control

Apache Software Foundation (ASF) telah merilis pembaruan keamanan untuk mengatasi kerentanan *SQL Injection* (CVE-2024-45387) pada Apache Traffic Control. Kerentanan ini memiliki skor CVSS 9.9, memungkinkan pengguna dengan peran tertentu, seperti 'admin' atau 'operations,' untuk mengeksekusi perintah SQL arbitrer pada *database* melalui permintaan PUT yang dirancang khusus. Apache Traffic Control telah memperbaiki kerentanan ini pada versi 8.0.2. Selain itu, ASF juga mengatasi kerentanan *bypass* autentikasi pada Apache HugeGraph-Server (CVE-2024-43441) dan kerentanan eksekusi kode jarak jauh (RCE) pada Apache Tomcat (CVE-2024-56337). Pengguna disarankan untuk segera memperbarui perangkat lunak mereka ke versi terbaru.

Prioritas : 2. Urgent

Sumber : https://thehackernews.com/2024/12/critical-sql-injection-vulnerability-in.html

Malwares

Malware 'OtterCookie' Baru Digunakan Sebagai *Backdoor*

Threat aktor Korea Utara menggunakan *malware* baru bernama OtterCookie dalam kampanye Contagious Interview yang menargetkan pengembang perangkat lunak dengan tawaran pekerjaan palsu. Kampanye ini, aktif sejak Desember 2022, awalnya menggunakan *malware* seperti BeaverTail dan InvisibleFerret, tetapi kini juga melibatkan OtterCookie yang diperkenalkan pada September 2023 dengan varian baru muncul pada November. OtterCookie disebarkan melalui *loader* yang mengeksekusi data JavaScript dari proyek Node.js atau paket npm yang diunduh dari GitHub atau Bitbucket, serta aplikasi berbasis Qt atau Electron. Setelah aktif, *malware* ini mencuri data penting seperti kunci dompet kripto, dokumen, gambar, hingga data clipboard, menggunakan komunikasi aman berbasis Socket.IO WebSocket. Variasi metode infeksi dan kemampuan baru menunjukkan eksperimen taktik oleh aktor ancaman di balik kampanye ini. Pengembang perangkat lunak disarankan berhati-hati terhadap tawaran kerja palsu, terutama yang melibatkan pengujian kode pada perangkat pribadi atau kerja.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/security/new-ottercookie-malware-used-to-backdoor-devs-in-fake-job-offers/

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