CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

6 Juni 2022

EDISI 098

OVERVIEW

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

General News

Microsoft Windows Autopatch Telah Tersedia Untuk Pratinjau Publik

Microsoft mengabarkan bahwa minggu ini Windows Autopatch, layanan untuk memperbarui perangkat lunak Windows dan Microsoft 365 secara otomatis di lingkungan perusahaan kini telah mencapai pratinjau publik. Layanan perusahaan ini pertama kali diumumkan pada bulan April ketika Redmond mengatakan akan tersedia secara umum pada Juli 2022 dan ditawarkan gratis kepada pelanggan Microsoft dengan lisensi Windows 10/11 Enterprise E3 atau lebih tinggi. Windows Autopatch secara otomatis mengelola penyebaran Windows 10 dan Windows 11 kualitas dan pembaruan fitur, *driver*, *firmware*, dan Aplikasi Microsoft 365 untuk pembaruan perusahaan. Langkah-langkah yang diperlukan untuk mendaftarkan pengguna pada pratinjau publik Windows Autopatch mengharuskan admin untuk masuk ke Endpoint Manager sebagai Administrator Global (Windows Autopatch di bawah menu Administrasi). Jika pengguna tidak melihat 'Windows Autopatch', maka pengguna tidak memiliki lisensi yang tepat. Lihat prasyarat Windows Autopatch untuk informasi selengkapnya tentang prasyarat, termasuk lisensi.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/microsoft/microsoft-windows-autopatch-now-available-for-public-preview/ >

Jutaan *Smartphone* Android Rentan Terkena Serangan Siber

Microsoft menyebut jutaan *smartphone* berbasis Android sangat berisiko untuk diretas. Raksasa teknologi asal AS itu mengklaim telah menemukan kerentanan keamanan baik di aplikasi yang ada di Play Store maupun di aplikasi bawaan. Tampaknya Play Protect yang selama ini digunakan Google untuk sistem operasi Android-nya sama sekali tidak mampu mengidentifikasi kerentanan. Untuk melindungi pengguna, pembaruan darurat telah tersedia dengan bantuan pakar Microsoft. Pihak Microsoft menjelaskan bahwa mereka melihat kerentanan dengan tingkat keparahan tinggi dalam kerangka kerja seluler milik mce Systems pada September 2021. Kerangka kerja yang dibuat sebelumnya ini memberikan kemudahan bagi pengembang dan untuk mengaktifkan perangkat Android. Namun, "kontrol ekstensif" dari produk yang disediakan oleh mce Systems menjadikannya target utama bagi peretas. Lebih lanjut kekurangan tersebut dapat memungkinkan *hacker* untuk menanamkan *backdoor* pada *smartphone* dari jarak jauh. Dengan *backdoor* ini, maka akan dapat menginstal virus atau *spyware* tanpa sepengetahuan korban. Lebih buruk lagi, seorang peretas dapat langsung mengambil kendali perangkat tanpa memerlukan akses fisik ke perangkat tersebut.

Prioritas: ***2. Urgent***

< https://www.idxchannel.com/economics/waspada-jutaan-smartphone-android-rentan-terkena-serangan-siber >

Breachs/Hacks/Leaks

Clipminer Meraup $1,7 Juta Dalam Penipuan Pembajakan Crypto

Malware tersebut, dijuluki Trojan.Clipminer yang memanfaatkan kekuatan komputasi dari sistem yang disusupi untuk menambang *cryptocurrency* serta mengidentifikasi alamat *crypto-wallet* dalam teks clipboard dan menggantinya untuk mengalihkan transaksi, menurut para peneliti dengan Tim Intelijen Ancaman Symantec. Sampel pertama *malware* ini muncul pada Januari 2021 dan mulai mempercepat penyebarannya pada bulan berikutnya hingga meraup 1,7 juta dolar dalam minggu ini. *Malware* tampaknya menyebar melalui unduhan trojan dari perangkat lunak *crack* atau bajakan. Clipminer menjatuhkan arsip WinRAR ke *host* dan secara otomatis mengekstrak dan menjatuhkan pengunduh dalam bentuk Dynamic Link Library (DLL). Setelah dieksekusi, kemudian menciptakan nilai registri dan mengganti namanya sendiri, memasukkannya ke dalam file sementara Windows. Dari sana *malware* mengumpulkan detail sistem dan menghubungkan kembali ke *command-and-control* server (C2) melalui jaringan Tor. *Malware* juga membuat scheduled *tasks* untuk memastikan sistem yang terinfeksi dan memperkecil kemungkinan file jahat lainnya muncul serta mengaburkan keberadaannya.

Prioritas: ***3. Important***

< https://www.theregister.com/2022/06/03/clipminer-cryptocurrency-millions/?&web_view=true >

Peretas Telah Mencuri Lebih Dari $250.000 Ethereum dari Bored Ape Yacht Club (BAYC)

Aktor ancaman mengkompromikan Bored Ape Yacht Club (BAYC) untuk ketiga kalinya tahun ini, mereka telah mencuri dan menjual NFT, menghasilkan 142 ETH, setara dengan lebih dari $250.000. Peretas melakukan serangan *phishing*, mereka membuat situs *phishing* yang meniru situs resmi BAYC dengan mengklaim bahwa pemegang BAYC, MAYC, dan OthersideMeta dapat mengklaim NFT gratis untuk waktu yang singkat. Situs web diiklankan melalui BAYC Discord resmi untuk manajer komunitas Yuga Labs yang sebelumnya diretas. Dalam serangan tersebut, EOA yang terkait dengan situs *phishing* diidentifikasi sebagai akun OpenSea EOA 0x1079061D37f7F3FD3295E4aAd02EcE4a3f20DE2d (sekarang diblokir). Setelah pencurian NFT, penyerang mulai menjual aset yang dikumpulkan pada 08:25:42 UTC. Setelah menjual NFT yang dicuri, pelaku ancaman memindahkan dana ke platform Tornado Cash.

Prioritas: ***3. Important***

< https://securityaffairs.co/wordpress/131950/hacking/bored-ape-yacht-club-hacked.html >

Vulnerabilities

Eksploitasi Dirilis Untuk *Bug* Atlassian Confluence RCE

Eksploitasi *proof-of-concept* untuk kerentanan kritis CVE-2022-26134 yang dieksploitasi secara aktif yang berdampak pada server Atlassian Confluence dan Data Center telah dirilis secara luas akhir pekan ini. Kerentanan yang dilacak sebagai CVE-2022-26134 adalah kerentanan *Remote Code Execution* (RCE) yang tidak diautentikasi kritis yang dieksploitasi melalui injeksi OGNL dan berdampak pada semua server Atlassian Confluence dan Data Center 2016 setelah versi 1.3.0. Eksploitasi yang berhasil memungkinkan penyerang jarak jauh yang tidak diautentikasi untuk membuat akun admin baru, menjalankan perintah, dan akhirnya mengambil alih server. Kerentanan itu diungkapkan minggu lalu setelah Volexity menemukan bahwa itu digunakan oleh banyak aktor ancaman dalam serangan. Pada saat itu, patch tidak tersedia, dan Atlassian menyarankan admin untuk membuat server *offline* atau memblokirnya agar tidak dapat diakses dari Internet.

Prioritas: ***1. Critical***

< https://www.bleepingcomputer.com/news/security/exploit-released-for-atlassian-confluence-rce-bug-patch-now/ >

Ponsel Motorola Berisiko Diretas dengan Kerentanan Pada Tingkat Chip

Salah satu chip perusahaan yang lebih tua ditandai sebagai vektor ancaman, menngakibatkan pemilik sejumlah ponsel murah dalam risiko dengan hanya beberapa prospek patch. Saat ini, terdapat kerentanan lain yang secara eksplisit memengaruhi chip Unisoc di tiga perangkat Motorola. Analis di Checkpoint Research telah menemukan kerentanan dalam chip Tiger T700 yang ada di perangkat Moto G20, E30, dan E40 tahun lalu. Tanpa terlalu teknis, kelemahan utamanya adalah tidak adanya pemeriksaan untuk memastikan bahwa pengendali koneksi modem membaca IMSI yang valid atau ID pelanggan serupa. Ketika *handler* membaca bidang nol-digit, *stack overflow* terjadi. Saat itulah terjadi serangan *Denial of Service* (atau eksekusi kode jarak jauh, jika dapat dieksploitasi).

Prioritas: ***2. Urgent***

< https://www.androidpolice.com/moto-g20-unisoc-tiger-t700-vulnerability/ >