www.idsirtii.or.id

09 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 209

OVERVIEW

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

General News

Amadey Bot Menyebarkan *Ransomware* LockBit 3.0 di Perangkat yang Diretas

Amadey Bot, *malware* yang digunakan untuk menginstal LockBit, didistribusikan melalui *file* dokumen Word berbahaya dan *executable* yang menyamarkan *icon file* Word. *File* berbahaya ini disebarkan menggunakan metode *phising.* Fungsi utama dari Amadey sendiri adalah untuk mengumpulkan informasi sensitif dari *host* yang terinfeksi atau sebagai saluran untuk mengirimkan artefak tahap berikutnya. Hasil analisis terbaru dari perusahaan keamanan siber pada *file* Microsoft Word yang diunggah ke VirusTotal menunjukkan bahwa dokumen tersebut berisi makro VBA berbahaya, yang ketika diaktifkan oleh korban, menjalankan perintah PowerShell untuk mengunduh dan menjalankan Amadey. Ketika Amadey berhasil dieksekusi, *malware* akan mengambil dan meluncurkan perintah tambahan dari server yang mencakup *ransomware* LockBit dalam format PowerShell (.ps1) atau biner (.exe).

Prioritas: ***1. Critical***

< https://thehackernews.com/2022/11/amadey-bot-spotted-deploying-lockbit-30.html >

Vultur Android *Banking Trojan* Mencapai Lebih Dari 100.000 Unduhan di Google Play Store

Vultur Android *Banking Trojan* telah mencapaitotal lebih dari 100.000 unduhan di Google Play Store. *Threat actor* juga menggunakan toko aplikasi resmi untuk mengirimkan *malware* menggunakan aplikasi *dropper. Dropper* bersembunyi di balik aplikasi utilitas palsu yang dapat menghindari langkah-langkah keamanan Goggle Play. Karena izinnya yang relatif terbatas dan jejak yang kecil, *dropper* muncul sebagai aplikasi sah dan dapat menghindari langkah-langkah keamanan Google Play. Secara teknis, setelah instalasi dilakukan, *dropper* menggunakan teknik penghindaran tingkat lanjut, termasuk steganografi, penghapusan *file,* dan obfuskasi kode. Setelah Vultur berhasil diinstal melalui pembaruan palsu, *threat actor* dapat mengamati semua yang terjadi pada perangkat terinfeksi dan melakukan penipuan bank melalui serangan pengambilalihan akun.

Prioritas: ***2. Urgent***

< https://www.infosecurity-magazine.com/news/vultur-android-banking-trojan/?&web_view=true >

Breachs/Hacks/Leaks

Maple Leaf Foods Kanada Terganggu oleh Serangan Siber

Maple Leaf Foods miliki Kanada telah mengonfirmasi bahwa mereka mengalami pemadaman listrik setelah menjadi korban serangan siber. Maple Leaf Foods sendiri memiliki lebih dari 14.000 karyawan dan menawarkan produk dengan berbagai merk, termasuk Maple Leaf, Schneiders, Mina, Greenfield Natural Meat Co., Lightlife, dan Field Roast. Perusahaan diketahui menjadi korban serangan siber yang mengakibatkan gangguan sistem tanpa membagikan rincian lebih lanjut tentang insiden. Maple telah mengambil tindakan dan melibatkan pakar keamanan siber dan pemulihan. Meskipun perusahaan belum memberikan rincian spesifik tentang serangan siber, diduga terdapat keterlibatan *ransomware* didalamnya.

Prioritas: ***3. Important***

< https://www.securityweek.com/cyberattack-causes-disruptions-canadian-meat-giant-maple-leaf-foods?&web_view=true >

Vulnerabilities

VMware Perbaiki Tiga *Auth Bypass Bug* pada *Remote Access Tool*

VMware telah merilis pembaruan keamanan untuk mengatasi tiga kerentanan dengan *critical severity* dalam Workspace ONE Assist yang memungkinkan penyerang jarak jauh melewati autentikasi dan meningkatkan hak istimewa ke admin. Kerentanan dilacak sebagai CVE-2022-31685 (autentikasi *bypass*), CVE-2022-31686 (metode autentikasi rusak), dan CVE-2022-31687 (kontrol autentikasi rusak) dengan skor CVSSv3 9,8/10. Penyerang tanpa autentikasi dapat mengeksploiyasinya dalam serangan dengan kompleksitas rendah yang tidak memerlukan interaksi pengguna untuk eskalasi hak istimewa. VMWare juga menambal kerentanan *cross-site scripting* (XSS) yang direfleksikan (CVE-2022-31688) yang memungkinkan penyerang untuk menyuntikkan kode Javascript di jendela pengguna target dan kerentanan *session fixation* (CVE-2022-31689) yang memungkinkan autentikasi setelah mendapatkan *session token* yang valid.

Prioritas: ***1. Critical***

< https://www.bleepingcomputer.com/news/security/vmware-fixes-three-critical-auth-bypass-bugs-in-remote-access-tool/ >

Microsoft Perbaiki Kerentanan Zero-Day ProxyNotShell Exchange

Microsoft telah merilis pembaruan keamanan untuk mengatasi dua kerentanan *zero-day* dengan *high severity* Microsoft Exchange yang dikenal sebagai ProxyNotShell. Kerentanan dilacak sebagai CVE-2022-41082 ddan CVE-2022-41040, memengaruhi Microsoft Exchange Server 2013, 2016, dan 2019. Penyerang dimungkinkan untuk meningkatkan hak istimewa dan menjalankan PowerShell dalam konteks sistem serta mendapatkan eksekusi kode arbitrer atau jarak jauh. Pembaruan dirilis secara kumulatif dalam Windows 11 KB5019980 dan KB5019961. Microsoft juga memantau deteksi yang sudah diterapkan ini untuk aktivitas jahat dan akan mengambil tindakan respons yang diperlukan untuk melindungi pelanggan. Perusahaan merilis langkah-langkah mitigasi untuk memungkinkan pemblokiran serangan ProxyNotShell yang masuk.

Prioritas: ***2. Urgent***

< https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-proxynotshell-exchange-zero-days-exploited-in-attacks/ >

Citrix Rilis Perbaikan Keamanan Kerentanan *Authentication Bypass*

Citrix telah merilis pembaruan keamanan untuk mengatasi kerentanan *authentication bypass* dengan *critical severity* pada Citrix ADC dan Citrix Gateway. Dalam pembaruannya, terdapat tiga kerentanan yang diatasi oleh perusahaan. Kerentanan pertama, yaitu CVE-2022-27510, kerentanan *authentication bypass* menggunakan jalur atau saluran alternatif yang memungkinkan penyerang mendapatkan akses tidak sah ke pengguna *Gateway*. Perusahaan menunjukkan bahwa hanya peralatan yang beroperasi sebagai *Gateway* (peralatan yang menggunakan fungsionalitas SSL VPN atau digunakan sebagai *proxy* ICA) yang terpengaruh. Kerentanan kedua, CVE-2022-27513, merupakan kerentanan verifikasi keaslian data yang memungkinkan penyerang melakukan pengambilalihan *remote desktop* melalui serangan *phising*. Kerentanan ini dapat dieksploitasi hanya jika perangkat dikonfigurasi sebagai VPN (*Gateway*) dan fungionalitas *proxy* RDP dikonfigurasi. Kerentanan lainnya, CVE-2022-27516, merupakan *bypass* fungsi perlindungan *brute-force login* pengguna yang hanya dapat dieksploitasi jika perangkat dikonfigurasi sebagai VPN (*Gateway*) atau server virtual AAA dengan konfigurasi “Max Login Attemps”. Perusahaan merekomendasikan untuk melakukan pembaruan ke versi terbaru sesegera mungkin.

Prioritas: ***1. Critical***

< https://securityaffairs.co/wordpress/138264/security/citrix-gateway-adc-flaws.html >