www.idsirtii.or.id

16 Juni 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 106

OVERVIEW

	General News	Breachs/Hacks/Leaks	Vulnerabilities
CRITICAL	0	0	3
URGENT	0	1	2
IMPORTANT	1	0	0

General News

Kampanye Peretasan Iran Melibatkan Duta Besar AS

Sekelompok peretas yang kemungkinan berafiliasi dengan Iran telah menjalankan kampanya *spear-phishing* yang melibatkan beberapa pejabat penting. Menurut laporan, para peretas Iran menyamar sebagai Mantan Duta Besar Amerika Serikat untuk menargetkan Ketua dari *mayor think tank*. Para peretas dapat memperoleh akses ke salah satu dari kontak *e-mail* target. Daftar target peretas termasuk di antaranya mantan pejabat Israel, personel militer berpangkat tinggi, kepala think tank keamanan terkemuka, dan Mantan Duta Besar AS untuk Israel. Laporan di Israel berspekulasi bahwa kampanye itu digencarkan oleh Fosfor, kelompok spionase dunia maya yang terhubung dengan Pemerintah Iran yang juga dikenal sebagai APT35, Newscaster Team, Charming Kitten, atau Magic Hound.

Prioritas: *3. Important*

< https://cyware.com/news/iranian-hacking-campaign-that-included-former-us-ambassador-1813699c >

Data Breach

Data Breach pada US *Ambulance Billing Service* Comstar Menyebabkan Kebocoran Data Kesehatan Pasien

Data Breach yang terjadi pada US *Ambulance Billing Service* Comstar berpotensi mengungkap informasi sensitif milik pasien. Insiden keamanan tersebut ditemukan pada 26 Maret, ketika Comstar melihat aktifitas mencurigakan pada beberapa server di dalam lingkungannya. Akibatnya, informasi sensitif seperti nama, tanggal lahir, informasi penilaian medis, pengobatan, dan asuransi kesehatan diakses oleh pihak yang tidak berwenang. Meskipun demikian, Comstar belum merilis informasi apa pun terkait dengan jumlah individu yang berpotensi terkena dampak tersebut, namun siapa pun yang dianggap terpengaruh dapat mengakses layanan *credit monitoring* secara gratis.

Prioritas: *2. Urgent*

< https://portswigger.net/daily-swig/data-breach-at-us-ambulance-billing-service-comstar-exposed-patients-healthcare-information?&web_view=true >

Vulnerabilities

Cisco Secure E-mail *Bug* Membiarkan Penyerang Melewati Otentikasi

Cisco memberikan peringatan kepada pengguna terkait dengan adanya kerentanan *critical* yang membiarkan penyerang melewati otentikasi dan dapat melakukan *login* ke antarmuka manajemen web milik Cisco. Kerentanan yang dilacak sebagai CVE-2022-20798 ditemukan dalam fungsi otentikasi eksternal dari Virtual and Hardware Cisco Email Security (ESA) dan Cisco Secure Email dan Web Manager Appliances. CVE-2022-20798 disebabkan oleh adanya pemeriksaan otentikasi yang tidak tepat pada perangkat yang menggunakan Lightweight Directory Access Protocol (LDAP) sebagai protocol autentikasi. Menurut Cisco, fitur otentikasi eksternal dinonaktifkan secara *default*, artinya hanya perangkat dengan konfigurasi *non-default* yang terpengaruh. Cisco juga mengatakan kerentanan ini tidak mempengaruhi produk Cisco Secure Web Appliance, yang sebelumnya dikenal sebagai Cisco Web Security Appliance (WSA).

Prioritas: *1. Critical*

< https://www.bleepingcomputer.com/news/security/cisco-secure-email-bug-can-let-attackers-bypass-authentication/ >

Bug Zimbra Mampu Mencuri *E-mail Logins* Tanpa Interaksi Pengguna

Telah ditemukan kerentanan tingkat tinggi pada *e-mail* Zimbra yang dapat dimanfaatkan oleh peretas untuk mencuri *login* tanpa adanya autentikasi pengguna. Masalah keamanan tersebut saat ini dilacak sebagai CVE-2022-27924 dan berdampak pada Zimbra 8.8.x dan 9.x untuk versi *open-source* dan *platform* komersial. Perbaikan

telah dipublikasikan untuk Zimbra versi ZCS 9.0.0 *Patch* 24.1 dan ZCS 8.8.15 *Patch* 31.1 yang sudah tersedia sejak 10 Mei 2022. Perbaikan tersebut membuat *hash* SHA -256 dari semua kunci Memcache sebelum dikirim ke *server.* Cacat tersebut telah dijelaskan dalam sebuah laporan dari para peneliti di SonarSource, yang merangkumnya sebagai "Memcached poisoning with an unauthenticated request." Eksploitasi dimungkinkan melalui injeksi CRLF ke dalam Memcached *Lookups.*

Prioritas: *1. Critical*

< https://www.bleepingcomputer.com/news/security/zimbra-bug-allows-stealing-email-logins-with-no-user-interaction/ >

Golang-based Peer-to-Peer (P2P) Botnet Menargetkan Server Linux

Dijuluki Panchan oleh Akamai *Security Research,* Botnet ini memperluas jangkauan dan fungsinya sebagai *cryptojacker* dan dirancang untuk membajak sumber daya komputer guna menambang *cryptocurrency.* Botnet penuh fitur yang bergantung pada *basic list of default* SSH ini melakukan Dictionary Attack. Panchan diketahui menyebarkan dan mengeksekusi dua *miner* yaitu XMRig dan nbhash pada *host* selama *runtime*. Perusahaan keamanan siber dan layanan *cloud* pertama kali melihat aktivitas Panchan pada 19 Maret 2022, dan mengaitkan *malware* tersebut dengan aktor ancaman dari Jepang.

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/06/panchan-new-golang-based-peer-to-peer.html?&web_view=true >

Kerentanan *Critical Code Execution* pada Splunk Enterprise

Splunk telah merilis *patch* 'out-of-band' yang mengatasi beberapa kerentanan di Splunk Enterprise, termasuk masalah kritis yang dapat menyebabkan *arbitrary code execution*. Dilacak sebagai CVE-2022-32158 dengan skor CVSS 9.0. merupakan kerentanan kritis yang baru ditangani karena Splunk Enterprise Deployment Server sebelum versi 9.0 memungkinakan klien untuk memanfaatkan *server* guna menyebarkan *forwader bundles* kepada klien lain. Hal ini dapat membahayakan Universal Forwader *endpoint* dan kemudian menyalahgunakannya untuk mengeksekusi kode arbitrer pada *endpoint* lain yang terhubung ke *deployment server.* Terkait dengan hal ini, perusahaan mengumumkan bahwa mereka telah menyelesaikan beberapa *bug* dengan tingkat keparahan tinggi pada Splunk Enterprise.

Prioritas: *1. Critical*

< https://www.securityweek.com/critical-code-execution-vulnerability-patched-splunk-enterprise?&web_view=true/ >

PureCrypter *Loader* Diperbaharui dengan Modul Baru

PureCrypter adalah *loader* dengan fitur lengkap yang dijual sejak Maret 2021 oleh aktor ancaman bernama 'PureCoder'. *Loader* ini ditulis dalam bahasa .NET serta menggunakan kompresi dan enkripsi untuk menghindari deteksi oleh perangkat lunak antivirus. PureCrypter diketahui masih dalam pengembangan dan sedang ditingkatkan dengan kemampuan baru untuk menargetkan lebih banyak entitas. Seperti yang diamati oleh ThreatLabz, PureCrypter telah digunakan untuk mendistribusikan berbagai *malware* termasuk AgentTesla, Arkei, AsyncRAT, Azorult, DcRAT, LokiBotStealer, Nanocore, RedLine Stealer, Remcos, Snake Keylogger, dan Warzone RAT. Baru-baru ini operator telah menambahkan fitur *loader malware* untuk menargetkan lebih banyak sumber daya. Tujuan utama dari *loader malware* adalah untuk mendistribusikan RAT dan pencuri informasi.

Prioritas: *2. Urgent*

< https://cyware.com/news/purecrypter-loader-updated-with-new-modules-1a0ba794 >