www.idsirtii.or.id

18 November 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 216

OVERVIEW

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

General News

Serangan Siber Lumpuhkan Vanuatu, Indonesia Dibawa-bawa

Serangan siber menghantam server dan telah melumpuhkan Vanuatu, memaksa pemerintah negara tersebut *offline* selama lebih dari 11 hari. Peretas telah menonaktifkan situs parlemen, polisi, dan kantor perdana menteri. Selain itu, serangan siber tersebut juga mematikan sistem *email*, intranet, dan *database online* sekolah, rumah sakit. Beberapa orang berspekulasi bahwa peretasan tersebut mungkin berasal dari Indonesia. Vanuatu telah lama mendukung gerakan kemerdekaan di provinsi Papua Barat, yang sebagian besar penduduknya adalah orang Melanesia. Militer Indonesia dituduh melakukan pelanggaran HAM berat di provinsi tersebut. Sementara itu Australia menawarkan bantuan untuk membangun kembali jaringannya. Sampai dengan Hari Rabu, domain pemerintah masih *down*. Seorang juru bicara mengatakan bahwa situs web tersebut harus kembali minggu depan.

Prioritas: *3. Important*

< https://international.sindonews.com/read/944813/40/serangan-siber-lumpuhkan-vanuatu-indonesia-dibawa-bawa-1668744717?showpage=all >

Indonesia Peringkat 3 Kebocoran Data

Indonesia menempati peringkat ketiga negara dengan kebocoran data terbanyak menurut studi perusahaan keamanan siber asal Belanda, Surfshark. Total, tingkat pelanggaran akun atau *account breach* pada kuartal III 2022 meningkat sebanyak 70 persen daripada kuartal II. Secara keseluruhan, total 108,9 juta akun di seluruh dunia dibobol selama kurun waktu Juli-September 2022. Pakar Keamanan Siber dari Vaksincom Alfons Tanujaya menjelaskan, data dalam laporan merupakan pelanggaran akun atau *account breach*. Sementara yang ramai selama ini di Indonesia, merupakan kebocoran *database* atau *database breach*. Alfons mengungkapkan, pelanggaran akun merupakan pembobolan terhadap berbagai macam akun, seperti Google, Facebook, Tokopedia, dan sejenisnya. Sedangkan database breach, tidak harus terhadap akun, meski berisi data sensitif seperti data kependudukan.

Prioritas: *3. Important*

< https://www.kompas.com/tren/read/2022/11/17/170500065/indonesia-peringkat-3-kebocoran-data-gara-gara-bjorka-?page=all#page2 >

Breachs/Hacks/Leaks

Kesalahan Konfigurasi pada *Server* yang Mengakibatkan PHI dari 600.000 Narapidana Terungkap

Kesalahan konfigurasi *server* di sebuah perusahaan yang menyediakan *medical claims processing* untuk fasilitas pemasyarakatan mengungkap informasi sensitif dari hampir 600.000 narapidana yang menerima perawatan medis selama dekade terakhir saat dipenjara. CorrectCare Integrated Health Inc. yang berbasis di Kentucky pada 31 Oktober melaporkan ke Departemen Kesehatan dan Layanan Kemanusiaan AS terkait dengan kebocoran data tersebut. Perusahaan mengatakan bahwa dua direktori file di *server* web CorrectCare telah secara tidak sengaja terungkap ke internet. Informasi pasien yang terdapat dalam direktori file yang terbuka termasuk nama lengkap, tanggal lahir, nomor Jaminan Sosial, dan informasi kesehatan terbatas, seperti kode diagnosis dan kode prosedur. Perusahaan mengatakan telah menerapkan langkah-langkah untuk meningkatkan keamanan sistemnya.

Prioritas: *2. Urgent*

< https://www.bankinfosecurity.com/misconfigured-server-exposed-phi-600000-inmates-a-20482?&web_view=true >

Vulnerabilities

Malware WASP Menggunakan Steganografi dan Polimorfisme

Malware yang dijuluki WASP menggunakan steganografi dan polimorfisme untuk menghindari deteksi dengan paket Python berbahaya yang dirancang untuk mencuri kredensial, informasi pribadi, dan mata uang kripto. Peneliti dari Phylum dan Check Point melaporkan melihat adanya paket berbahaya baru di PyPI. Analis di Checkmarx mengatakan operator tersebut masih merilis paket berbahaya. Laporan Checkmarx merinci ratusan infeksi yang berhasil dari *infostealer malware* WASP, dan menemukan sejumlah fitur menarik untuk menghindari alat keamanan siber.

Prioritas: *2. Urgent*

< https://www.theregister.com/2022/11/16/wasp_python_malware_checkmarx/?&web_view=true >

Peneliti Rapid7 Mengidentifikasi Beberapa Kerentanan yang Memengaruhi Produk F5

Peneliti Rapid7 menemukan beberapa kerentanan pada perangkat F5 BIG-IP dan BIG-IQ yang menjalankan *customized distribution* CentOS. Para ahli juga menemukan beberapa jalan pintas dari kontrol keamanan yang tidak dikenali oleh vendor keamanan F5 sebagai kerentanan yang dapat dieksploitasi. Kerentanan yang ditemukan oleh para ahli adalah CVE-2022-41622 dan CVE-2022-41800. CVE-2022-41622 adalah eksekusi kode melalui *Cross-site Request Forgery* (CSRF) yang berdampak pada produk BIG-IP dan BIG-IQ. CVE-2022-41800 adalah eksekusi kode jarak jauh melalui RPM *spec injection* yang berada dalam mode Appliance iControl REST. Kerentanan tersebut telah dinilai sebagai kerentanan dengan tingkat keparahan tinggi. Rapid7 melaporkan kedua kerentanan tersebut ke F5 pada 18 Agustus 2022 dan mendukung vendor yang menanganinya.

Prioritas: *2. Urgent*

< https://securityaffairs.co/wordpress/138631/security/2-rce-f5-products.html?web_view=true >

Beberapa Grup Menghancurkan Situs *Web E-Commerce* dengan Serangan TrojanOrder

Menurut peneliti Sansec, ada lonjakan besar dalam serangan TrojanOrders menjelang musim liburan dan sekitar 38% situs web Magento 2 dan Adobe Commerce menjadi sasaran serangan tersebut. Penyerang menginfeksi situs dengan JavaScript berbahaya

yang mencuri informasi pelanggan dan nomor kartu kredit saat membeli produk di toko *online*. Meskipun Adobe memperbaiki kerentanan yang dieksploitasi pada bulan Februari, eksploitasi PoC tersedia untuk waktu yang lama dan peneliti mengklaim setidaknya sepertiga dari semua toko Magento dan Adobe Commerce belum ditambal sejauh ini. Peretas sering memanfaatkan kerentanan yang dapat dieksploitasi untuk meluncurkan serangan yang berhasil demi keuntungan finansial. Pengguna disarankan untuk memperbarui sistem secara teratur.

Prioritas: *2. Urgent*

< https://cyware.com/news/multiple-groups-tear-down-e-commerce-websites-with-trojanorder-attacks-e8224917 >