www.idsirtii.or.id

1 Desember 2022

CYBER BLITZ

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 225

OVERVIEW

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

General News

Kota Batu Bentuk CSIRT untuk Antisipasi Ancaman Siber

Pemerintah Kota Batu, Jawa Timur meluncurkan Batu Kota *Computer Security Incident Response Team* (CSIRT) atau tim tanggap insiden siber guna mewaspadai adanya ancaman siber pada lingkup pemerintahan. Wali Kota Batu Dewanti Rumpoko mengatakan bahwa insiden keamanan siber bisa terjadi kapan saja dan menimbulkan kerugian serius pada institusi pemerintahan. Pembentukan tim ini bekrjasama dengan Badan Siber dan Sandi Negara (BSSN). Kota Batu menjadi kota ke-29 yang meluncurkan CSIRT dari 514 kabupaten kota seluruh Indonesia. Dengan terbentuknya tim itu, diharapkan mengatasi berbagai permasalahan keamanan informasi pada layanan berbasis elektronik di Pemerintah Kota Batu.

Prioritas: *3. Important*

< https://cyberthreat.id/read/14905/Kota-Batu-Bentuk-CSIRT-untuk-Antisipasi-Ancaman-Siber >

Australia Mengesahkan Peraturan Pemberian Denda hingga AU$50 Juta Kepada Perusahaan Yang Mengalami *Data Breach*

Pemerintah Australia telah mengeluarkan undang-undang yang mengatur perusahaan yang mengalami *data breach* yang berulang dan dinilai serius. Denda maksimum yang akan diberikan sebesar AU$50 juta, 30% dari omzet dalam periode insiden, atau tiga kali lipat nilai kerugian yang disebabkan dari insiden data breach yang dialami, dipilih dari ketiga opsi itu yang memiliki nilai paling besar. Periode yang dimaksud adalah jangka waktu sejak *data breach* terjadi sampai dengan akhir bulan ketika insiden tersebut selesai ditangani. Undang-undang ini tersebut muncul dilatarbelakangi adanya insiden *data breach* yang menimpa Optus dan Medibank yang mengakibatkan kebocoran informasi pribadi dengan masing-masing sejumlah 2,1 juta dan 9,7 juta data pelanggan.

Prioritas: *3. Important*

< https://thehackernews.com/2022/11/australia-passes-bill-to-fine-companies.html >

Peretas Korea Utara Menggunakan *Backdoor* "Dolphin" Baru untuk Memata-matai Korea Selatan

Kelompok kejahatan siber ScarCruft dari Korea Utara telah dikaitkan dengan *backdoor* yang belum terdokumentasi yang disebut Dolphin. *Backdoor* ini digunakan untuk menargetkan Korea Selatan. Kampanye tersebut, pertama kali ditemukan oleh Kaspersky dan Volexity tahun lalu. ScarCruft, juga disebut APT37, InkySquid, Reaper, dan Ricochet Chollima. Kelompok kejahatan siber ini merupakan kelompok yang bermotivasi geo-politik dengan rekam jejak menyerang entitas pemerintah, diplomat, dan organisasi berita yang terkait dengan urusan Korea Utara, kelompok ini diketahui sudah aktif setidaknya sejak 2012. Apa yang membuat Dolphin jauh lebih berbahaya daripada *backdoor* lainnya adalah kemampuannya untuk mendeteksi *removable device* dan melakukan ekstraksi file seperti media, dokumen, email, dan sertifikat.

Prioritas: *1. Important*

< https://thehackernews.com/2022/12/north-korea-hackers-using-new-dolphin.html >

Breachs/Hacks/Leaks

Peretas Spionase dari China Menggunakan Perangkat USB untuk Menargetkan Entitas di Filipina

Pelaku kejahatan siber yang diduga merupakan kelompok Nexus dari China telah dikaitkan dengan serangkaian serangan spionase di Filipina. Mereka memanfaatkan perangkat USB sebagai vektor infeksi awal. Mandiant, yang merupakan bagian dari Google Cloud, sedang melakukan analisis artefak yang digunakan dalam intrusi menunjukkan bahwa kampanye serangan tersebut telah berlangsung sejak September 2021. Salah satu, firma intelijen ancaman dan respons insiden mengatakan bahwa serangan tersebut menyebabkan penyebaran tiga keluarga malware baru yang dijuluki MISTCLOAK, DARKDEW, dan BLUEHAZE. Penggunaan drive USB untuk menyebarkan malware bukan merupakan hal baru. Worm Raspberry Robin diketahui juga menggunakan drive USB sebagai titik masuk infeksi.

Prioritas: *1. Important*

< https://thehackernews.com/2022/11/chinese-cyber-espionage-hackers-using.html >

Vulnerabilities

Peretas Saat Ini Aktif Mengeksploitasi Kerentanan Produk Fortinet

Pada saati ini telah terdeteksi aktifitas para pelaku kejahatan siber sedang aktif melakukan eksploitasi pada kerentanan pada produk Fortinet. Kerentanan tersebut merupakan kerentanan *bypass* autentikasi, didefinisikan sebagai CVE-2022-40684, dengan skor CVSS 9,6, kerentan ini berdampak pada berbagai versi Produk Fortinet, termasuk FortiOS, FortiProxy, dan FortiSwitchManager. Menurut peneliti Cyble, kerentanan ini mempengaruhi FortiOS versi 7.2.0 hingga 7.2.1, FortiOS versi 7.0.0 hingga 7.0.6, FortiProxy versi 7.2.0, FortiProxy versi 7.0.0 hingga 7.0.6, FortiSwitchManager versi 7.2.0, dan FortiSwitchManager versi 7.0.0. Kerentanan ini memungkinkan penyerang tanpa melakukan autentikasi mendapatkan akses lengkap ke sistem yang ditargetkan, melakukan operasi pada antarmuka administratif melalui permintaan HTTP atau HTTPS, dan berinteraksi dengan semua *endpoint* API manajemen. Para peneliti menemukan bahwa terdapat lebih dari seratus ribu firewall FortiGate yang terhubung langsung ke internet dimana hal tersebut sangat berpotensi dieksploitasi oleh peretas.

Prioritas: *1. Critical*

< https://cyware.com/news/hackers-actively-abuse-vulnerability-in-fortinet-products-ba3911bf >

Kerentanan Baru Berdampak Pada Produk OT Festo dan CODESYS

Para peneliti telah mengungkapkan secara detail celah kerentanan baru yang berdampak pada produk teknologi operasional (OT) dari CODESYS dan Festo yang dapat menyebabkan *source code tampering* dan penolakan layanan (DoS). Kerentanan, yang dilaporkan oleh Forescout Vedere Labs ini merupakan kerentanan yang terbaru dari daftar panjang kelemahan yang telah ditemukan. Kerentanan yang paling berdampak buruk adalah CVE-2022-3270 (skor CVSS: 9,8). Kerentanan ini berdampak pada produk pengontrol otomasi Festo, dimana peretas dapat menggunakan protokol Festo Generic Multicast (FGMC) untuk mem-boot ulang perangkat tanpa memerlukan autentikasi apa pun dan dapat menyebabkan penolakan layanan (DoS). Kerentanan lainnya berdampak pada produk CODESYS. Kerentanan ini terkait dengan penggunaan kriptografi yang lemah pada lingkungan runtime CODESYS V3, didefinisikan sebagai CVE-2022-4048 (skor CVSS: 7.7) kerentanan ini dapat dimanfaatkan oleh penyerang untuk memanipulasi *source code.*

Prioritas: *2. Urgent*

< https://thehackernews.com/2022/11/3-new-vulnerabilities-affect-ot.html >