'Cyber blitz.
www.idsirtii.or.id

DIREKTORAT OPERASI KEAMANAN SIBER

EDISI 219 | 29 Nopember 2024

OVERVIEW	Critical	Urgent	Important
General News	0	0	1
Breachs/Hacks/Leaks	0	2	0
Vulnerabilities	0	3	0
Malwares	0	2	0

General News

Apakah Tenaga Kerja Keamanan Siber Sudah Memuncak?

Analisis tenaga kerja terbaru dari ISC2 telah memicu reaksi keras karena fokusnya pada kesenjangan antara jumlah profesional keamanan siber yang dibutuhkan dan perkiraan tenaga kerja saat ini. Para kritikus berpendapat bahwa fokus pada kesenjangan tersebut bukanlah ukuran permintaan yang sebenarnya, dan bahwa kurangnya anggaran untuk membayar tenaga kerja keamanan siber telah menyebabkan stagnasi permintaan profesional keamanan siber. Meskipun 59% profesional yang disurvei oleh ISC2 mengaku membutuhkan pekerja terampil, bisnis masih membelanjakan anggaran mereka di tempat lain, yang mengakibatkan stagnasi pasar untuk talenta keamanan siber.

Prioritas : 3. Important
Sumber : https://www.darkreading.com/vulnerabilities-threats/cybersecurity-workforce-peaked

Breachs/Hacks/Leaks

Geico dan Traveler Didenda $11,3 Juta karena Lemahnya Keamanan Data

New York telah memerintahkan dua perusahaan asuransi mobil, Government Employees Insurance Co (GEICO) dan Travelers Indemnity Co, untuk membayar $11,3 juta atas praktik keamanan yang tidak sesuai yang memungkinkan para peretas membobol data pribadi lebih dari 12.000 penduduk. Kedua perusahaan asuransi tersebut terbukti melanggar peraturan negara bagian untuk melindungi data konsumen dan lembaga keuangan. GEICO diperintahkan untuk membayar $9,75 juta, sementara Travelers akan membayar $1,55 juta. Kedua perusahaan tersebut terbukti melanggar peraturan negara bagian untuk menerapkan kebijakan, prosedur, dan kontrol yang dirancang untuk melindungi data konsumen dan lembaga keuangan. Perusahaan-perusahaan asuransi tersebut telah setuju untuk meningkatkan praktik keamanan siber mereka, termasuk meningkatkan perlindungan terhadap informasi pribadi, melakukan inventarisasi data yang komprehensif, mewajibkan otentikasi,

menerapkan pencatatan dan pemantauan, dan meningkatkan perencanaan respons terhadap ancaman.

Prioritas : 2. Urgent
Sumber : https://www.darkreading.com/cybersecurity-operations/geico-travelers-fined-lax-data-security

Banshee Stealer Menutup Operasi Setelah Source Code Bocor

Malware macOS malware-as-a-service Banshee Stealer telah dihapus setelah kode sumbernya bocor secara online dan dipublikasikan di GitHub oleh VXunderground. Malware yang menargetkan x86_64 dan ARM64 ini sebelumnya dilaporkan memungkinkan kompromi data sistem, dompet mata uang kripto, peramban, dan ekstensi peramban secara ekstensif. Operator di balik Banshee Stealer telah menutup operasi mereka setelah kebocoran data tersebut.

Prioritas : 2. Urgent
Sumber : https://insight.scmagazineuk.com/infostealer-shut-down-after-source-code-was-leaked

Vulnerabilities

Kerentanan pada HPE Insight Remote Support

HPE telah mengeluarkan buletin keamanan darurat yang membahas kerentanan kritis dalam layanan Insight Remote Support. Kerentanan tersebut, dengan skor CVSS setinggi 9,8, dapat memungkinkan penyerang mendapatkan akses tidak sah ke informasi sensitif atau mengeksekusi kode berbahaya dari jarak jauh. Kerentanan tersebut meliputi kelemahan XML External Entity Injection, kelemahan Java Deserialization, dan kerentanan Directory Traversal. HPE telah merilis Insight Remote Support v7.14.0.629. Pengguna disarankan untuk segera memperbarui instalasi mereka untuk mengurangi risiko eksploitasi. Untuk mengakses perangkat lunak terbaru, pengguna dapat menavigasi ke Pengaturan Administrator> Pembaruan Perangkat Lunak di dalam aplikasi. HPE merekomendasikan penginstalan perangkat lunak terbaru yang tersedia secara otomatis.

Prioritas : 2. Urgent
Sumber :https://securityonline.info/hpe-insight-remote-support-hit-with-critical-vulnerabilities-urgent-patch-released/

Beberapa Kerentanan Ditemukan pada Jenkis Automation Server

Jenkins, server otomatisasi sumber terbuka, telah mengeluarkan peringatan keamanan yang membahas beberapa kerentanan pada sistem inti dan pluginnya. Kelemahan ini, termasuk penolakan layanan dan skrip lintas situs, menimbulkan risiko yang signifikan bagi pengguna Jenkins jika tidak ditambal. Kerentanan penolakan layanan (CVSS 7.5) telah diidentifikasi dalam pustaka pemrosesan JSON Jenkins, yang memungkinkan penyerang dengan izin Keseluruhan/Baca untuk membuat permintaan HTTP yang menangani utas sibuk tanpa batas waktu, menyebabkan waktu henti yang signifikan. Peringatan ini juga menyoroti plugin yang memungkinkan penyerang yang tidak memiliki izin Overall/Read untuk melakukan hal yang sama, seperti SonarQube Scanner dan Bitbucket. Kerentanan XSS tersimpan dengan tingkat keparahan tinggi (CVSS 8.0) telah ditemukan di Plugin Antrian Sederhana, yang memungkinkan penyerang menyuntikkan skrip berbahaya yang dapat

dieksekusi oleh pengguna lain. Plugin Parameter Daftar Sistem Berkas juga mengandung kerentanan (CVSS 4.3) yang memungkinkan penyerang untuk menghitung nama file pada sistem file pengontrol Jenkins. Jenkins telah merilis versi terbaru untuk mengatasi kerentanan ini, dan mendesak pengguna untuk segera melakukan upgrade.

Prioritas : 2. Urgent
Sumber : https://securityonline.info/jenkins-users-beware-multiple-security-vulnerabilities-discovered/

Kerentanan pada Zabbix yaitu CVE-2024042327

Zabbix, alat pemantauan infrastruktur TI sumber terbuka, telah ditemukan memiliki kerentanan injeksi SQL yang kritis (CVE-2024-42327). Kerentanan ini memungkinkan penyerang untuk meningkatkan hak istimewa dan mendapatkan kendali atas instance Zabbix, yang berpotensi membahayakan data pemantauan sensitif dan sistem yang terhubung. Kerentanan ini terletak di titik akhir API user.get dan dapat dieksploitasi oleh pengguna non-admin mana pun dengan akses API, termasuk mereka yang memiliki peran "Pengguna" default. Eksploitasi yang berhasil dapat menyebabkan pelanggaran data, kompromi sistem, dan penolakan layanan. Zabbix telah mengatasi kerentanan pada versi 6.0.32rc1, 6.4.17rc1, dan 7.0.1rc1, dan organisasi disarankan untuk memperbarui penerapannya ke versi tambalan terbaru serta meninjau peran dan izin pengguna untuk memastikan hanya personel yang berwenang yang memiliki akses API.

Prioritas : 2. Urgent
Sumber : https://securityonline.info/cve-2024-42327-critical-sql-injection-vulnerability-found-in-zabbix/?

Malwares

Hacktivist Pro-Rusia Luncurkan Operasi Ransomware as a Service

CyberVolk, sebuah kelompok hacktivist pro-Rusia, telah meluncurkan operasi ransomware-as-a-service (RaaS) miliknya sejak Juni 2024. Kelompok ini, yang berasal dari India, telah mengaku bertanggung jawab atas beberapa serangan ransomware antara bulan Juni dan Oktober. CyberVolk juga telah mempromosikan dan berbagi perangkat dengan ransomware family lainnya. Analisis ini menyoroti semakin kaburnya batas antara hacktivisme, kejahatan siber, dan aktivitas negara-bangsa. CyberVolk telah menjadi pemain penting dalam ekosistem kejahatan siber, menggunakan serangan DDoS dan menggunakan kembali malware komoditas yang sudah ada. Kelompok ini mengklaim beraliansi dengan kelompok hacktivist dan kejahatan siber, termasuk Lapsus$ dan Moroccan Dragons. Versi modifikasi ransomware CyberVolk menggunakan muatan khusus Windows yang ditulis dalam bahasa C++, yang menghentikan proses yang sedang berjalan milik Microsoft Management Console atau Task Manager. CyberVolk baru-baru ini menggunakan muatan ransomware bermereknya dalam serangan terhadap berbagai entitas di Jepang, termasuk Badan Meteorologi Jepang (JMA) dan Pusat Sistem Informasi Global Tokyo. Kasus CyberVolk menunjukkan sifat dinamis dari afiliasi dan aliansi di antara kelompok-kelompok peretas, sehingga lebih menantang bagi para pembela siber untuk melacak aktivitas mereka secara konsisten.

Prioritas : 2. Urgent
Sumber : https://www.infosecurity-magazine.com/news/russian-hacktivists-branded/

Kelompok Penyerang APT-C-60 Menargetkan Jepang Menggunakan Platform Tepercaya

Sebuah serangan siber yang menargetkan organisasi Jepang dan Asia Timur, yang diduga didalangi oleh APT-C-60, telah ditemukan. Serangan ini melibatkan email phishing yang menyamar sebagai lamaran pekerjaan, memperkenalkan malware melalui tautan berbahaya yang dihosting di platform yang sah seperti Google Drive. Serangan dimulai dengan tautan Google Drive, mengunduh file VHDX yang berisi file pintasan LNK berbahaya. Malware tersebut kemudian menggunakan string data yang disandikan dan kunci XOR untuk mengaburkan operasi komunikasi dan muatannya. Malware pintu belakang, SpyGrace, diidentifikasi sebagai varian 3.1.6. JPCERT memperingatkan organisasi untuk memantau saluran perekrutan, meneliti tautan yang tidak diminta, dan menerapkan mekanisme deteksi ancaman tingkat lanjut untuk memitigasi risiko serupa.

Prioritas : 2. Urgent
Sumber : https://www.infosecurity-magazine.com/news/aptc60-targets-japan-using-trusted/

Ditandatangani secara elektronik oleh:
DIREKTUR OPERASI KEAMANAN SIBER

Andi Yusuf, M.T.
Pembina Utama Muda (IV/c)

KONTAK KAMI

DEPUTI BIDANG OPERASI KEAMANAN SIBER DAN SANDI
NATIONAL CSIRT OF INDONESIA
Id-SIRTII/CC
INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE COORDINATION CENTER

@Id_SIRTII (+62) 811 1065 2018 bantuan70@bssn.go.id