'Cyber blitz.
www.idsirtii.or.id
DIREKTORAT OPERASI KEAMANAN SIBER
EDISI 150 | 21 AGUSTUS 2023

| OVERVIEW | Critical | Urgent | Important |
|---|---|---|---|
| *General News* | 0 | 1 | 1 |
| *Breachs/Hacks/Leaks* | 0 | 2 | 1 |
| *Vulnerabilities* | 1 | 0 | 0 |
| *Malwares* | 0 | 1 | 0 |

## *General News*

### *Security Update* Perangkat Keras Jaringan Juniper OS untuk Mengatasi Kerentanan Kritikal

Perusahaan teknologi perangkat keras Juniper Network telah merilis pembaruan keamanan untuk 4 (empat) kerentanan pada komponen J-Web Junos OS. Kerentanan tersebut dapat berdampak pada *remote code execution* (RCE) dengan nilai CVSS kumulatif 9.8 (kritikal). Keempat kerentanan tersebut dilacak sebagai CVE-2023-36844, CVE-2023-36845, CVE-2023-36846, dan CVE-2023-36847. Kerentanan tersebut telah diatasi dalam versi Seri EX (Junos OS versi 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S4, 22.1R3-S3, 22.2R3-S1, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3, dan 23.2R1) dan Seri SRX (Junos OS versi 20.4R3-S8, 21.2R3-S6, 21.3R3-S5, 21.4R3-S5, 22.1R3-S3, 22.2R3-S2, 22.3R2-S2, 22.3R3, 22.4R2-S1, 22.4R3, dan 23.2R1).

Prioritas : 2. Urgent
Sumber : https://thehackernews.com/2023/08/new-juniper-junos-os-flaws-expose.html

### Google Mengembangkan Ekstensi untuk Mendeteksi Ekstensi *Malicious*

Google sedang mengembangkan dan menguji fitur baru pada Browser Chrome yang berfungsi untuk mendeteksi ekstensi yang telah dihapus dari Chrome Web Store yang diinstal pada browser. Penghapusan ekstensi biasanya menunjukkan bahwa ekstensi tersebut merupakan *malicious extension* atau *malware*. Ekstensi berupa *malware* biasanya dibuat oleh perusahaan *scam* dan *threat actor* untuk menyisipkan iklan serta melacak riwayat. Ekstensi tersebut tetap terinstal meskipun telah dihapus dari Store, oleh karena itu fitur Safety Check ini dikembangkan. Fitur ini akan aktif di Chrome 117 dan saat ini dapat diuji pada Chrome 116.

Prioritas : 3. Important

Sumber : https://www.bleepingcomputer.com/news/google/google-chrome-to-warn-when-installed-extensions-are-malware/

## *Breachs/Hacks/Leaks*

### Gang Ransomware Kuba Menargetkan Organisasi Infrastruktur dan Perusahaan IT dengan Kerentanan Veeam Backup & Replication

Peneliti ancaman BlackBerry mendeteksi aktivitas Gang Ransomware Kuba sejak awal Juni 2023. Gang Ransomware Kuba menargetkan organisasi infrastruktur di Amerika Serikat dan Perusahaan IT di Amerika Latin. Gang tersebut memanfaatkan kerentanan CVE-2023-27532 pada produk Veeam Backup & Replication (VBR) untuk mencuri kredensial dari file konfigurasi. Gang Ransomware Kuba diindikasikan merupakan aktor ancaman dari Rusia, hal tersebut didasarkan pada pengecualian infeksi pada komputer yang menggunakan pola *keyboard* Rusia.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/security/cuba-ransomware-uses-veeam-exploit-against-critical-us-organizations/

### APT Bronze Starlight Menggunakan Sertifikat Penyedia VPN untuk Menandatangani Aplikasi Malware

Peneliti keamanan SentinelLabs mengamati aktivitas Grup APT (Advanced Persistent Threat) Bronze Starlight yang diindikasikan terkait dengan aktor China. Aktivitas Grup tersebut menargetkan industri perjudian di Asia Tenggara dengan menggunakan *malware* yang ditandatangani menggunakan sertifikat valid milik PMG PTE LTD yang merupakan penyedia VPN Ivacy di Singapura. Penggunaan sertifikat valid bertujuan untuk menghindari deteksi perimeter keamanan sehingga aplikasi dapat berjalan sacara sah.

Prioritas : 2. Urgent
Sumber : https://www.bleepingcomputer.com/news/security/hackers-use-vpn-providers-code-certificate-to-sign-malware/

### Threat Actor Rusia Memanfaatkan Aplikasi Obrolan Zulip untuk Peretasan Diplomatik

Peneliti keamanan EclecticIQ menemukan kampanye *spear-phishing* yang sedang berlangsung yang dilakukan oleh pelaku ancaman yang terkait dengan Rusia dan menargetkan Kementerian Luar Negeri negara-negara yang tergabung dalam NATO. Para ahli mendeteksi dua file PDF yang menyamar sebagai berasal dari kedutaan besar Jerman dan berisi dua umpan undangan diplomatik. Pelaku ancaman menggunakan aplikasi obrolan Zulip untuk C&C (*command and control*) dalam kampanye ini.

Prioritas : 3. Important
Sumber : https://cyberthreat.id/read/15880/Peretas-Rusia-Gunakan-Aplikasi-Obrolan-Zulip-untuk-Serangan-Phishing-Diplomatik

## Vulnerabilities

### Kerentanan Remote Code Execution pada Aplikasi WinRAR

Peneliti keamanan Zero Day Initiative (ZDI) menemukan celah kerentanan pada aplikasi WinRAR yang dapat berdampak pada *remote code execution* (RCE). Kerentanan tersebut dilacak sebagai CVE-2023-40477 dengan nilai CVSS 7.8. RARLAB selaku pengembang aplikasi telah melakukan pembaruan aplikasi WinRAR pada versi 6.23. Para pengguna WinRAR disarankan segera memperbarui ke versi 6.23 untuk menghindari kemungkinan dampak yang dapat terjadi.

Prioritas : 1. Critical
Sumber : https://www.techworm.net/2023/08/winrar-remote-hackers-execute-arbitrary-code.html

## Malwares

### Sebanyak 3.300 Aplikasi Android Menggunakan Metode Kompresi Tidak Biasa untuk Menghindari Analisis

Peneliti keamanan Zimperium zLab mengklaim mendeteksi sebanyak 3.300 aplikasi Android (APK) menggunakan metode anti-analisis yang tidak biasa. File APK yang menggunakan format ZIP hanya mendukung 2 metode yaitu tanpa kompresi (metode STORED) dan menggunakan algoritma kompresi (DEFLATE). Aplikasi ini belum ditemukan pada Google Play Store namun dapat berfungsi dengan baik pada Android versi 9 dan yang terbaru.

Prioritas : 2. Urgent
Sumber : https://www.liputan6.com/tekno/read/5375259/3300-aplikasi-apk-android-pakai-trik-curang-ini-agar-tak-terhendus-polisi-siber

KONTAK KAMI

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

@Id_SIRTII (+62) 21 7883 3610 bantuan70@bssn.go.id