LAPORAN PENANGANAN KEJADIAN DAN INSIDEN SIBER

Nomor Dokumen: LPI-SI/2026/03/001

Tanggal Laporan: 6 Juli 2026

Klasifikasi: Internal

A. Ringkasan Eksekutif (*Executive Summary*)

Telah terjadi upaya serangan *brute force* yang menargetkan sistem autentikasi (halaman login) website utama yang beralamat di https://rsudsoeselo.tegalkab.go.id. Sistem keamanan berbasis *Web Application Firewall* (WAF) dari Wordfence berhasil mendeteksi dan memblokir serangkaian percobaan login yang gagal dari beberapa alamat IP yang tersebar di Amerika Serikat, Singapura, dan Indonesia. Penyerang menggunakan metode otomatis untuk menebak kredensial dengan memasukkan kombinasi *username* acak dan umum secara berulang-ulang. Sistem pertahanan berfungsi dengan baik memblokir IP tersebut, dan langkah selanjutnya yang diperlukan adalah penguatan aturan login (Hardening) untuk mencegah serangan serupa di masa mendatang.

B. Detail Insiden

Jenis Insiden: *Brute Force Attack* (Percobaan Login Tidak Sah)
Target Serangan: Halaman Login Administrator/Pengguna
Sistem Pertahanan Aktif: Wordfence Security Plugin
Status Saat Ini: Serangan berhasil diblokir sementara oleh sistem *lockout* Wordfence.
Data IP Penyerang Teratas:

- 5.253.84.92 (Amerika Serikat) – 15 kali diblokir
- 62.60.130.103 (Amerika Serikat) – 7 kali diblokir
- 94.237.65.225 (Singapura) – 6 kali diblokir
- 135.136.39.36 (Amerika Serikat) – 2 kali diblokir
- 140.213.200.238 (Indonesia) – 1 kali diblokir

C. Kronologi Kejadian (*Timeline*)

1. Sistem WAF mencatat lonjakan aktivitas lalu lintas masuk yang tidak wajar pada parameter login.
2. Terjadi puluhan permintaan (*requests*) login dari 5 alamat IP berbeda (3 IP asal AS, 1 IP asal Singapura, 1 IP asal Indonesia).
3. Penyerang secara berurutan mencoba masuk menggunakan daftar *username* tebakan, yaitu: bot (4 kali), admin (4 kali), root (3 kali), aios (2 kali), dan a123456 (2 kali).
4. Wordfence mendeteksi bahwa *username* yang dicoba tersebut **tidak terdaftar di database sistem** (*Existing User: No*).
5. Berdasarkan ambang batas kegagalan login (*failed login threshold*), sistem langsung melakukan blokir (Total 31 tindakan pemblokiran teratas telah dieksekusi).

D. Dampak Insiden

1. I**ntegritas Data & Kredensial: AMAN**. Tidak ada akun yang berhasil dibobol karena seluruh *username* yang digunakan penyerang bukan merupakan pengguna yang valid di dalam sistem.
2. **Ketersediaan (Availability) & Performa Server:** Terdapat beban *resource* (CPU/RAM) tambahan yang minimal untuk memproses *request login* dan eksekusi pemblokiran oleh Wordfence, namun operasional website tidak terganggu.

E. Tindakan Penanganan & Mitigasi

Sesuai instruksi untuk eskalasi penanganan, tindakan berikut akan segera diterapkan:

1. **Eksekusi Pemblokiran Permanen (Permanent Blacklist):** Mengambil daftar IP dari tabel "Top 5 IPs Blocked" (5.253.84.92, 62.60.130.103, 94.237.65.225, 135.136.39.36, 140.213.200.238) dan

memasukkannya ke dalam opsi *Blocking/Banning* secara permanen melalui menu *Update Blocked IPs*.

2. **Pemblokiran Berbasis Geografis (Geo-Blocking - Opsional):** Mengingat lalu lintas anomali terbesar berasal dari Amerika Serikat (24 blokir) dan Singapura (6 blokir), pemblokiran akses halaman login dari negara tersebut dapat dipertimbangkan jika website difokuskan hanya untuk akses administratif dari wilayah lokal (Indonesia).

F. Akar Masalah (*Root Cause Analysis*)

1. Serangan ini murni dilakukan oleh *botnet* otomatis atau *script* eksploitasi yang secara acak memindai (*crawling*) URL login standar di internet.
2. *Bot* mengandalkan *dictionary attack* menggunakan *username* bawaan/default CMS (seperti admin, root) untuk mencari celah pada website yang administratornya belum mengubah kredensial bawaan.
3. Kebijakan *Brute Force Protection* yang berjalan saat ini masih mengizinkan beberapa kali percobaan sebelum IP akhirnya diblokir.

G. Rekomendasi & Langkah Pencegahan (*Post-Incident Action*)

Untuk mengubah dan memperketat aturan *Brute Force Protection* ke depannya, implementasikan langkah berikut pada menu *Update Login Security Options*:

1. **Perketat Parameter *Lockout*:**
    - Turunkan jumlah *Lockout after how many login failures* (Misalnya: dari 10 atau 5 menjadi **3 percobaan gagal**).
    - Tingkatkan durasi pemblokiran IP (Misalnya: dari 5 menit menjadi **2 bulan** atau **permanen** untuk pelanggar berulang).
2. **Pemblokiran Langsung (*Immediate Ban*):**
    - Aktifkan opsi: *"Immediately block the IP of users who try to sign in as these usernames"*.

- Masukkan daftar username bodong yang sering dicoba *bot* ke dalam kolom tersebut: admin, root, bot, aios, a123456, administrator. Siapapun yang mencoba login dengan nama tersebut akan langsung diblokir permanen di percobaan pertama.

3. **Penguatan Lanjutan (Bila diperlukan):**
   - Wajibkan penggunaan Autentikasi Dua Faktor (2FA) untuk seluruh akun yang memiliki hak akses modifikasi ke dalam sistem (administrator/editor).
   - Terapkan *IP Whitelisting* jika akses administratif hanya dilakukan dari jaringan kantor pemerintahan atau IP statis yang sudah dikenali.

H. Penutup & Otorisasi

Pelapor	Kepala IT
	
Indra Purwa Laksana, S.Kom	Teguh Wawang Erawan, S.Kom

Ketua CSIRT

Kepala Dinas Kominfo Kab. Tegal