# FORM REKAP INSIDEN

| No. Dokumen. | Kategori Dokumen | Tanggal Efektif |
|---|---|---|
| 500.12.10.1/34/01/2024 | Terbatas | 5 June 2024 |
| | Versi | Update Terakhir |
| | 1.1 | 1-Sep-26 |

| Disusun Oleh | Diperiksa Oleh | Disahkan Oleh |
|---|---|---|
| Tim SMKI | CISO | Manajemen Puncak |
| Ervin Sandy Saputra | Andi Hermanto,S.Kom., M.Eng | Aris Pramana, S.E. M.M. |

| No | Tanggal Pelaporan | Penerima Laporan | Nama Pelapor | Tanggal Insiden | Kategori Insiden | Deskripsi | Domain/ Sub domain | Analisis Penyebab |
|---|---|---|---|---|---|---|---|---|
| 500.12.10.1/34/01/01/2026 | 9 Januari 2026 | Ervin Sandy | Hernanda | 9 Januari 2026 | Medium Impact | Reflected Cross-Site Scripting (XSS) pada parameter item di endpoint /2020/galleries/read pada modul galeri. | blud.klaten.go.id | Parameter item direfleksikan ke respons tanpa sanitasi/encoding yang memadai sehingga input dapat dieksekusi oleh browser. |
| 500.12.10.1/34/01/02/2026 | 17 Januari 2026 | Ervin Sandy | Ahmad Reza Aulia Siregar | 17 Januari 2026 | Low Impact | Stored HTML Injection pada field Slug di halaman /settings. Input HTML dapat tersimpan dan dirender kembali pada halaman profil/menu akun. | bayat.klaten.go.id | Input pengguna belum difilter/disanitasi dan output belum dilakukan HTML encoding sebelum ditampilkan kembali ke browser. |
| 500.12.10.1/34/01/03/2026 | 16 Februari 2026 | Ervin Sandy | Primandito Adi Setiya | 16 Februari 2026 | High Impact | Sensitive Data Exposure pada endpoint /rest/settings yang dapat diakses publik tanpa autentikasi dan menampilkan kredensial/API key. | x.disbudporapar.klaten.go.id | Endpoint konfigurasi REST dapat diakses tanpa autentikasi sehingga informasi sensitif terekspos ke publik. |
| 500.12.10.1/34/01/04/2026 | 12 Maret 2026 | Ervin Sandy | Putra | 12 Maret 2026 | Medium Impact | SNMP Information Disclosure: layanan SNMP dengan community string "public" terekspos ke internet publik. | 103.108.187.1 | Security misconfiguration pada perangkat jaringan yang mengizinkan akses SNMP dari internet publik. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 500.12.10.1/34/01/05/2026 | 28 April 2026 (metadata dokumen) | Ervin Sandy | Anggito Dirgantoro | 28 April 2026 (metadata dokumen) | High Impact | Tiga temuan pada aplikasi vendor: IDOR pada detail penyedia, default/weak credential akun superadmin, dan information disclosure pada endpoint API. | vendor.klaten.go.id | Kontrol otorisasi objek belum memadai, autentikasi admin lemah, serta perlindungan endpoint API dan pembatasan percobaan login belum mencukupi. |
| 500.12.10.1/34/01/06/2026 | 6 Mei 2026 (metadata dokumen) | Ervin Sandy | Rakha Hayya Ilhamsyah | 6 Mei 2026 (metadata dokumen) | High Impact | Broken Access Control pada tautan Google Drive di halaman BKPSDM: akses umum "Anyone with the link" memberikan peran Editor kepada pengguna anonim. | bkpsdm.klaten.go.id / Google Drive publik | Kesalahan konfigurasi izin berbagi cloud storage sehingga folder resmi yang seharusnya read-only dapat diedit oleh publik. |
| 500.12.10.1/34/01/07/2026 | 13 Juni 2026 | Tim CSIRT Kabupaten Klaten | Badan Siber dan Sandi Negara (BSSN) | 5 Mei s.d. 3 Juni 2026 | High Impact | BSSN mendeteksi komunikasi beberapa aset jaringan Pemerintah Kabupaten Klaten dengan Indicator of Compromise (IoC) yang berkaitan dengan aktivitas Generic Trojan RAT. | Jaringan 103.108.187.0/24 (aset Diskominfo Klaten) | Terdeteksi komunikasi DNS ke IP yang dinilai malicious dan berelasi dengan file trojan. Infeksi pada host masih memerlukan verifikasi dan investigasi lebih lanjut. |
| 500.12.10.1/34/01/08/2026 | 26 Juli 2026 | Ervin Sandy | Akbar Hidayat Husain | 26 Juli 2026 | High Impact | Website compromise melalui SEO cloaking/conditional content injection: halaman sidiklat menampilkan konten judi online ketika diakses menggunakan User-Agent Googlebot, sedangkan pengguna normal melihat halaman biasa. | sidiklat.bkpsdm.klaten.go.id | Indikasi modifikasi tidak sah pada sisi server; dugaan penyebab meliputi injeksi/modifikasi file aplikasi atau .htaccess, remote script loader, dan kemungkinan backdoor ter-obfuscate. |
| 500.12.10.1/34/01/09/2026 | 15 Agustus 2026 | Ketua CSIRT Kabupaten Klaten | Abdurrohman Haadziq (melalui BSSN) | 13 Agustus 2026 | Medium Impact | BSSN memvalidasi kerentanan Exposed Administrative Interface pada domain pemerintahan.klaten.go.id melalui path /cpanel dan /controlpanel. | pemerintahan.klaten.go.id | Antarmuka administrasi dapat diakses dari internet publik sehingga layanan administrasi terekspos sebagai permukaan serangan. |

| Dampak Insiden | Tindak Lanjut | Tanggal Mulai | Tanggal Selesai | PIC Perbaika | Status | Pembelajaran dari Insiden |
|---|---|---|---|---|---|---|
| Risiko pencurian sesi, phishing/manipulasi tampilan, dan pengalihan pengguna ke situs berbahaya. | Validasi input parameter item dan terapkan output encoding (misalnya htmlspecialchars) sebelum data ditampilkan ke browser. | 17 Januari 2026 | 17 Januari 2026 | Herlan | Close | Validasi input dan output encoding harus diterapkan secara konsisten pada parameter yang ditampilkan kembali. |
| Manipulasi konten/defacement serta risiko phishing dan social engineering melalui tautan yang disisipkan. | Melakukan HTML encoding sebelum menampilkan data pengguna dan memastikan karakter khusus dikonversi menjadi entitas HTML. | 29 Januari 2026 | 29 Januari 2026 | Yasin | Close | Terapkan sanitasi input dan output encoding pada setiap data yang berasal dari pengguna. |
| Akses tidak sah ke sistem internal, kompromi integritas data, dan potensi eskalasi serangan ke sistem lain. | Endpoint telah terpantau menjadi 404 pada tindak lanjut 16 Februari 2026. Tetap perlu rotasi seluruh kredensial/API key yang terekspos, audit log akses, dan review endpoint REST lainnya. | 16 Februari 2026 | 17 Februari 2026 | Yasin | Close | Endpoint konfigurasi dan secret tidak boleh terekspos publik; kredensial yang pernah terekspos harus segera dirotasi. |
| Informasi topologi jaringan, interface, tabel routing, dan spesifikasi OS perangkat dapat dipetakan pihak luar dan dimanfaatkan untuk serangan lanjutan. | Nonaktifkan akses SNMP dari internet publik atau batasi dengan IP whitelisting hanya untuk server monitoring internal. | 12 Maret 2026 | 12 Maret 2026 | Yasin | Close | Protokol manajemen jaringan harus dibatasi ke jaringan/IP tepercaya dan tidak diekspos langsung ke internet. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Paparan data vendor, potensi pengambilalihan akun superadmin/kendali aplikasi, serta pemetaan endpoint/teknologi internal. | Terapkan pengecekan hak akses (RBAC), gunakan identifier yang sulit ditebak, reset kredensial admin, aktifkan MFA, rate limiting/CAPTCHA, dan lindungi seluruh endpoint API dengan autentikasi. | 28-Apr-26 | 29-Apr-26 | Yasin | Close | Otorisasi harus diverifikasi pada setiap request; akun admin wajib memakai autentikasi kuat dan endpoint API harus terlindungi. |
| Pihak luar dapat mengunggah/mengubah file, menyisipkan malware atau phishing, memalsukan informasi resmi, dan menyalahgunakan ruang penyimpanan. | Ubah akses umum dari "Editor" menjadi "Viewer", audit isi folder, dan hapus file/folder asing yang tidak berasal dari pihak internal. | 6 mei 2026 | 7 mei 2026 | Yasin | Close | Tautan dokumen publik harus menggunakan prinsip least privilege dan secara berkala diaudit agar hanya memiliki akses lihat/unduh. |
| Jika infeksi terkonfirmasi, RAT dapat memungkinkan akses jarak jauh, pencurian data/kredensial, kerusakan sistem, instalasi malware tambahan, cryptomining, dan penyebaran ke perangkat lain. | Verifikasi log traffic/CPU/proses, lakukan forensik pada host terindikasi, update antivirus dan sistem, deep scanning, hapus program/file berbahaya, reset kredensial, perkuat IDS/IPS/firewall, dan lakukan pemantauan jaringan proaktif | 13 Juni 2026 | 13 Juni 2026 | Yasin | Close | Anomali komunikasi ke IoC perlu dipantau proaktif dan segera ditindaklanjuti dengan verifikasi host, forensik, serta penguatan perimeter. |
| Penyalahgunaan domain resmi, kerusakan reputasi, risiko de-index/blacklist mesin pencari, serta potensi phishing, malware, dan akses persisten penyerang. | Periksa integritas file terhadap source asli, identifikasi dan hapus backdoor/loader, audit permission upload/write, serta analisis log historis untuk menemukan aktivitas mencurigakan. | 26 Juli 2026 | 27 Juli 2026 | Yasin | Close | Pemulihan tampilan saja tidak cukup pada kasus compromise; perlu pemeriksaan integritas, backdoor, permission, dan log untuk memastikan akses penyerang benar-benar terputus. |
| Paparan antarmuka administrasi ke internet publik dengan tingkat severity Medium berdasarkan hasil validasi BSSN. | Lakukan validasi/verifikasi aset terdampak, remediasi aplikasi/layanan yang mengekspos antarmuka administrasi, kemudian laporkan hasil remediasi kepada BSSN. | 15 Agustus 2026 | 16 Agustus 2026 | Yasin | Close | Antarmuka administrasi sebaiknya tidak diekspos publik tanpa pembatasan akses dan harus menjadi bagian dari pemeriksaan rutin permukaan serangan. |