

	b. Compromised Account adalah kondisi ketika akun pengguna telah diambil alih atau dikendalikan oleh pihak yang tidak sah. Hal ini bisa terjadi akibat leaked credentials atau serangan lain seperti: Phishing berhasil (korban memberikan kredensial secara sukarela); Serangan session hijacking atau token theft; Eksploitasi kelemahan autentikasi (misalnya tidak ada MFA); dan Malware yang mencuri cookie sesi atau data login.
Dampak	: - Penyerang dapat menggunakan data tersebut untuk mencoba login (<i>credential stuffing</i>); - Potensi akses tidak sah ke berbagai layanan lain (karena password reuse); - Meningkatnya risiko pencurian data pribadi dan <i>identity theft</i>; - Penyalahgunaan identitas digital; - Akses ke data sensitif organisasi; - Penyebaran malware atau penipuan menggunakan akun yang tampak sah; dan - Potensi merusak reputasi institusi.
Proof of Concept	: 1. Penyerang/<i>threat actor</i> berhasil masuk ke Sistem Informasi Dinas Perpustakaan dan Arsip Daerah DIY dengan kredensial yang didapatkan melalui <i>malware</i>, <i>social engineering</i>, <i>keylogger</i> dll. Setelah berhasil masuk maka username/password tersebut dijual belikan di forum <i>dark web</i>. 2. Aplikasi atau URL yang username/password nya diindikasikan bocor: - https://arsip.jogjaprovo.go.id/ - https://dpad.jogjaprovo.go.id/ - https://dioramaarsip.jogjaprovo.go.id/home - https://jogjabelajar.jogjaprovo.go.id/ - https://balaiyanpus.jogjaprovo.go.id/

Screenshots

1. Contoh Data username/password yang tersebar di dark web/breach forum:

1220104	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	ariyantowahyudi111@gmail.com
1.95E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	853-5791-3132
1.96E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	Azzalati653@gmail.com
1.99E+15	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	muga
1.97E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	
9.88E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	
admin_respati	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	ucup123456789
1.98E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	aufisekargalih@gmail.com
1.96E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	adziasalsabita.8989@student.uny.ac.id
1.96E+17	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	valentinobisaya18
amsafdy	Mar 3rd, 2025	Ganja Cloud		balayampus.jogiaprov.go.id	indrabiyon@gmail.com
3.4E+15	Mar 3rd, 2025	DataLeak2025		balayampus.jogiaprov.go.id	devalentin2303
rgasetrum@gmail.com	Mar 3rd, 2025	RedCloud URL:LOG-PASS		balayampus.jogiaprov.go.id	asmulfauz3@gmail.com
erika_pp	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	delaapril453@gmail.com
3.4E+15	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	
1.98E+17	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	
idgolo	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	ari.pustro@jogiaprov.go.id
1.97E+17	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	art.siswo@gmail.com
2021_tani	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	
Syafiq_NW	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	
64645459	Mar 3rd, 2025	Evil Data Parser - ULP BASE / Combo		balayampus.jogiaprov.go.id	
marcmaref@vfr.fr	Mar 3rd, 2025	TKT LOG url:loginpass COMBO LOGS		balayampus.jogiaprov.go.id	sulph16@gmail.com
atvnc	Mar 3rd, 2025	TKT LOG url:loginpass COMBO LOGS		balayampus.jogiaprov.go.id	
terencecm	Mar 3rd, 2025	TKT LOG url:loginpass COMBO LOGS		balayampus.jogiaprov.go.id	rahmaniyusu96@gmail.com
baru	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	
baru	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	
tom	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	UCUP123456789
yogitama	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	rahmaniyusu96
yogitama	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	rahmaniyusu96@gmail.com
CONDUCTOR	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id	UCUP123456789
tom	Mar 3rd, 2025	Moon Cloud Combo/htbases		balayampus.jogiaprov.go.id/admin/login	admin@tlab.co.id

ADHUIASA	3.4E+15	Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	zakhyandri09@gmail.com
		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
	3.4E+15	Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
admin		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
BDMYATI		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
tapadhita@gmail.com		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	
disperindag		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	tiket
panduan		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id	tiket
PKL2022		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	mgdlnaria8@gmail.com
	3401082004	Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	daniawita.dia@gmail.com
mitrasibakul		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	yulirismati@gmail.com
panel@ibakul.com		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	rahaelgalang19@gmail.com
	3402	Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	zakhyandri09@gmail.com
rizd.yuda@gmail.com		Feb 20th, 2025	AZUL CLOUD	dioramaansip.jogiaprov.go.id/home	axelmhrdn@gmail.com

	1.97E+17	Feb 20th, 2025	AZUL CLOUD	dpad.jogiaprov.go.id/users/admin/login	franzhendrikus@gmail.com
	1.99E+17	Feb 20th, 2025	AZUL CLOUD	dpad.jogiaprov.go.id/users/admin/login	frbzhezhdrukus@gmail.com
	1.99E+17	Feb 20th, 2025	AZUL CLOUD	dpad.jogiaprov.go.id/users/admin/login	franzhendrikus

Rekomendasi

Perbaikan

1. Melakukan validasi dan konfirmasi terhadap informasi yang disampaikan kepada Dinas Komunikasi dan Informatika DIY;
2. Memberikan kesadaran keamanan terhadap pengguna akhir terhadap jenis kelemahan yang ditemukan, dalam rangka meningkatkan *Security Awareness* khususnya edukasi pengguna tentang phishing dan keamanan akun;
3. Melakukan audit forensik dan IT *Security Assessment* terhadap akun-akun yang diduga leak secara berkala dan berkesinambungan;
4. Mengupayakan deteksi perilaku anomali (*anomaly detection*) pada sistem login;
5. Wajibkan reset password setelah insiden terdeteksi;
6. Memberlakukan kebijakan untuk tidak menggunakan password yang sama pada aplikasi-aplikasi/website yang digunakan;
7. Segera mencabut semua sesi aktif dan token autentikasi yang tersimpan;

	8. Implementasi MFA / step-up authentication pada login dari perangkat baru; 9. Menerapkan penggunaan antivirus, melakukan penggantian <i>Password</i> pada akun-akun yang telah <i>leak</i> , serta menerapkan <i>multi-factor authentication</i> ; dan 10. Menonaktifkan URL aplikasi yang sudah tidak dipergunakan
Referensi	: - https://owasp.org/Top10/A03_2021-Injection/ - https://owasp.org/Top10/A09_2021-Security_Logging_and_Monitoring_Failures/ - https://owasp.org/Top10/A01_2021-Broken_Access_Control/ - https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/ - https://owasp.org/Top10/A02_2021-Cryptographic_Failures/

Dapat kami sampaikan bahwa untuk meminimalisir dampak lanjutan, sementara sistem informasi tersebut akan kami lakukan pembatasan akses jika tidak ada tindak lanjut/konfirmasi dari Dinas Perpustakaan dan Arsip Daerah DIY, Sehubungan dengan hal tersebut, dimohon kepada Kepala Dinas Perpustakaan dan Arsip Daerah Istimewa Yogyakarta untuk:

1. Memerintahkan tim teknis segera melakukan perbaikan dan rekomendasi diatas supaya tidak menimbulkan dampak lebih lanjut;
2. Menunjuk PIC untuk segera mengkonfirmasi terkait status Sistem Informasi yang terdampak dan menyampaikan rencana penanggulangan insiden tersebut kepada Dinas Komunikasi dan Informatika DIY; dan
3. Menginformasikan progres perbaikannya kepada Dinas Komunikasi dan Informatika DIY.

selanjutnya untuk koordinasi dan konfirmasi, dapat menghubungi Dinas Komunikasi dan Informatika DIY melalui nara hubung Saudara Anik Budiati (0899-6626-663) / Ari Widiyatmoko(0857-2935-4200) atau melalui *channel* aduan Discord pada *link* berikut: <https://s.id/discord-diskominfo-diy>.

Demikian kami sampaikan, atas perhatiannya kami ucapkan terima kasih.

KEPALA,

HARI EDI TRI WAHYU NUGROHO, S.I.P., M.Si.

Salinan Untuk DPAD DIY