Security Incident Report

Report Date: March 16, 2026
Classification: Internal

Incident ID: **INC-2026-0847** HIGH SEVERITY

Detected:	Mar 15, 2026 14:23 UTC	**Resolved:**	Mar 15, 2026 18:47 UTC
Duration:	4 hours 24 minutes	**Status:**	RESOLVED
Reporter:	Monitoring System (automated)	**Lead:**	Alex Rivera, Security Team

AFFECTED SYSTEMS

System	Impact	Status
API Gateway (api.pressa.dev)	High	Restored
Authentication Service	Medium	Restored
User Database (Primary)	Medium	Restored

INCIDENT SUMMARY

An unauthorized access attempt was detected on the API Gateway at 14:23 UTC. The attacker exploited a misconfigured rate limiting rule to perform credential stuffing against the authentication endpoint. Approximately 12,400 login attempts were made from a distributed botnet spanning 847 unique IP addresses. No user accounts were compromised. The attack was detected by the anomaly detection system and mitigated through automated IP blocking and manual rule updates.

TIMELINE OF EVENTS

- **14:23** — Anomaly detection triggers alert: unusual login attempt volume detected
- **14:31** — Security team acknowledges incident, begins investigation
- **14:45** — Attack vector identified as credential stuffing via distributed botnet
- **15:12** — Automated blocking enabled, 847 IPs added to blocklist
- **16:30** — Rate limiting rules updated and hardened
- **18:47** — Full service restoration confirmed, incident closed

REMEDIATION ACTIONS

Action	Owner	Status
Deploy enhanced rate limiting rules	A. Rivera	Complete
Implement CAPTCHA on login after 3 failures	M. Chen	In Progress
Audit all API endpoints for similar vulnerabilities	J. Park	In Progress
Update incident response playbook	A. Rivera	Pending