SAMPLE - FICTIONAL - NOT A REAL INCIDENT

IronWiFi FedRAMP 20x sample: Ongoing Incident Report (IEC-CSO-OIR)

> SAMPLE - FICTIONAL - NOT A REAL INCIDENT. Illustrative format example only, published in the IronWiFi Trust Center for FedRAMP 20x review. Does not describe any real IronWiFi, customer, tenant, employee or federal agency event. IronWiFi is pursuing FedRAMP 20x Class A and is not FedRAMP Certified.

Human-readable twin of `fedramp-20x-sample-incident-report-ongoing.json`. Both files follow the FedRAMP Incident Report JSON Schema `fedramp-incident-report-schema-2026-06-24.json` (version 0.2.1, https://www.fedramp.gov/schemas/fedramp-incident-report-schema-2026-06-24.json). Rules: https://www.fedramp.gov/2026/reference/20x/b/incident-evaluation-and-communication/

Report issued (fictional): 2026-03-13T18:00:00Z

Report header

Schema field	Value
`reportType`	Ongoing
`providerTrackingId`	SAMPLE-IR-2026-0001-FICTIONAL
`certificationPackageOverviewUri`	https://www.ironwifi.com/fedramp/ironwifi-fedramp-public.json
`federalIncidentCoordinator`	SAMPLE ONLY: Jane Q. Coordinator <federal-ir-coordinator@example.com>; +1-555-0100 (unchanged)

1. Incident description (`incidentDescription`)

SAMPLE - FICTIONAL - NOT A REAL INCIDENT. A staging support-console misconfiguration allowed an unauthorized engineering role to run read-only queries against RADIUS authentication-event metadata (usernames, device identifiers, NAS identifiers, timestamps; no passwords, EAP secrets, shared secrets or private keys) for one fictional federal pilot tenant (agency.example.gov). Access was limited to a US-region analytics replica. Treated as a FedRAMP Reportable Incident under IEC-CSO-EFR because confidentiality of federal customer data was potentially affected. Update: access window confirmed as about 42 minutes (14:05Z to 14:47Z) by one engineering identity; no evidence of external exfiltration.

2. Timeline (`timeline`)

SAMPLE - FICTIONAL

Schema field	Value
`startedAt`	2026-03-12T14:05:00Z
`detectedAt`	2026-03-12T14:38:00Z
`detectionSource`	SAMPLE: Privileged-access monitoring alert on the staging support console (fictional alert rule SAMPLE-PRIV-QUERY-SPIKE)
`evaluationCompletedAt`	2026-03-12T15:10:00Z

`occurredAt`	`milestoneDescription`
2026-03-12T14:05:00Z	SAMPLE: Misconfiguration introduced during a fictional staging role-template change.
2026-03-12T14:38:00Z	SAMPLE: Detection via privileged-access monitoring; on-call engineer paged.
2026-03-12T14:55:00Z	SAMPLE: Role revoked; misconfigured template rolled back; affected queries stopped.
2026-03-12T15:10:00Z	SAMPLE: FedRAMP reportability evaluation completed (possible confidentiality impact; integrity and availability not indicated).
2026-03-12T16:00:00Z	SAMPLE: Initial Incident Report (IEC-CSO-IIR) issued.
2026-03-13T18:00:00Z	SAMPLE: Review of query logs completed; no external destinations observed. Ongoing Incident Report (IEC-CSO-OIR) issued.

3. Potential Agency Impact N-rating (PAIN), IEC-CSO-EFI (`potentialImpact`)

Schema field	Value
`historicalRating`	3, 2
`currentRating`	2
`evaluationNotes`	SAMPLE IEC-CSO-EFI: Initially PAIN-3. Reduced to PAIN-2 (likely narrow customer effect) after log review showed no external destinations and access limited to one engineering identity for about 42 minutes.

4. Functional impact (`functionalImpact`)

SAMPLE: Potential confidentiality impact to authentication-event metadata for one fictional federal pilot tenant. No integrity impact to RADIUS/802.1X authentication decisions. No availability impact. Impacted data types (fictional): usernames, device identifiers, NAS identifiers, timestamps. Not

SAMPLE - FICTIONAL

impacted: passwords, EAP method secrets, RADIUS shared secrets, private keys, payment data. Update: no evidence that any data left the staging environment.

5. Recovery plan (`recoveryPlan`)

SAMPLE (updated): Steps 1 and 2 complete. Step 3, the automated role-template check, in review, estimated 2026-03-14. Step 4, recovery verification and Final Incident Report, estimated 2026-03-14.

6. Likely affected customer agencies (`affectedAgencies`)

- SAMPLE ONLY: Fictional Pilot Agency (agency.example.gov), NOT a real agency (unchanged)

7. Observed incident activity (`observedActivity`)

SAMPLE IEC-CSO-OIR: Between 2026-03-12T14:05Z and 14:47Z one engineering identity (engineer.sample@example.com) issued 17 read-only SELECT queries against the staging auth-events replica, all matching one fictional tenant_id SAMPLE-TENANT-0001. No write, delete, export or cross-tenant queries observed.

8. Indicators of compromise (`indicatorsOfCompromise`)

- `Source IP 192.0.2.45 (TEST-NET-1 documentation range; fictional office egress)` (sample)
- `User-Agent curl/8.5.0 (scripted API client)` (sample)
- `Role grant ID SAMPLE-ROLE-GRANT-9f3a` (sample)
- `Query fingerprint SELECT username, calling_station_id, nas_identifier, event_time FROM auth_events WHERE tenant_id=...` (sample)

9. Related CVE identifiers (`relatedCveIds`)

None. Configuration defect; no CVE applies.

10. Root cause (`rootCause`)

SAMPLE: The staging IAM role template omitted an environment guard, so a role intended for synthetic test tenants also matched the fictional federal pilot tenant replica. Configuration defect; no CVE applies.

11. Response and recovery activities (`responseAndRecoveryActivities`)

SAMPLE: Role revoked and prior template restored; query audit logs preserved; outbound destinations reviewed with none found outside staging; fictional agency contact notified through its agency-specific channel; regression check drafted.

Notification parties (sample)

Under the IEC-CSO rules a real report goes to FedRAMP (fedramp_security@fedramp.gov), to affected agencies through their own incident reporting procedures, and to all necessary parties as

SAMPLE - FICTIONAL

an update in the provider's Trust Center. This sample was not sent to FedRAMP's security inbox or to any agency; it is published only as a format example.

End of SAMPLE - FICTIONAL - NOT A REAL INCIDENT.

SAMPLE - FICTIONAL