MALICIOUS 92/100

Dormant IAM user svc-backup-legacy disabled Block Public Access and set a Principal:* read policy on customer-data bucket example-corp-customer-exports from unrecognized datacenter infrastructure - anonymous reads occurred during a 41-minute exposure window; disable the key, restore the policy, and audit accessed objects now.

HOST AWS account 111122223333 (production), region us-east-1

USER **svc-backup-legacy**

TIME **2026-07-09T09:34:41Z**

MITRE **T1078.004 (Valid Accounts: Cloud Accounts), T1530 (Data from Cloud Storage), T1562.007 (Impair Defenses: Disable Cloud Firewall / Access Controls)**

SEVERITY CRITICAL

Org: ORG001 · Alert ORG001-AWS-1 · Generated 2026-07-09T10:42:17Z

EXECUTIVE SUMMARY

This alert is a true positive exposure of customer data. The IAM user `svc-backup-legacy` - inactive for 63 days, no MFA, access key unrotated for 311 days - executed a short reconnaissance sequence and then, within 90 seconds, disabled Block Public Access on `example-corp-customer-exports` and applied a bucket policy granting `s3:GetObject` to `Principal: *`. The bucket holds 18,442 objects of customer CSV exports. All API calls originated from `198.51.100.77`, a datacenter-hosted IP never before associated with this identity, whose historical usage is exclusively from the VPC NAT range used by the retired backup pipeline. S3 server access logs confirm 3 anonymous `GET` requests from 2 external IPs during the 41-minute exposure window before responders re-enabled Block Public Access at 10:15Z. CloudTrail data events were not enabled on the bucket, so the anonymous-read count is a lower bound. The access key must be disabled immediately, the exposure treated as a reportable data incident pending object-level audit, and the credential-leak source hunted, since dormant-key use from foreign infrastructure indicates the key was stolen, not misused internally.

ALERT DETAILS

CREATED AT	2026-07-09T09:34:41Z
HOST	AWS account `111122223333` (production), region us-east-1
USER	IAM user `svc-backup-legacy` (access key `AKIAIOSFODNN7EXAMPLE`; no MFA; dormant 63 days)
SEVERITY	CRITICAL
MITRE	T1078.004 (Valid Accounts: Cloud Accounts), T1530 (Data from Cloud Storage), T1562.007 (Impair Defenses: Disable Cloud Firewall / Access Controls)
PATTERN	Recon (GetCallerIdentity, ListBuckets) followed by PutPublicAccessBlock and PutBucketPolicy within 90 seconds from a first-seen ASN

BUCKET	`example-corp-customer-exports` - 18,442 objects (~92 GB) of customer CSV exports; tagged `data-classification: restricted`
POLICY CHANGE	Block Public Access disabled (all four settings), then bucket policy granting `s3:GetObject` to `Principal: *` on `arn:aws:s3:::example-corp-customer-exports/*`
SOURCE IP	`198.51.100.77` (ASN 64510 - Example Datacenter Corp; 21/93 VirusTotal; first-seen for this identity and this account)
EXPOSURE WINDOW	41 minutes (09:34:12Z policy applied to 10:15:27Z Block Public Access restored)
GUARDDUTY	`Policy:S3/BucketBlockPublicAccessDisabled` and `Policy:S3/BucketAnonymousAccessGranted` fired on the same events; `UnauthorizedAccess:IAMUser/InstanceCredentialExfiltration` not triggered (key is a long-lived IAM key, not instance role)
PRIOR CASES	No prior cases for this identity or bucket; 1 unrelated benign case for planned public website bucket (ORG001-AWS-0412)

INVESTIGATION QUESTIONS

What exactly changed, and does the new configuration expose customer data?

• Both protective layers were removed in sequence: Block Public Access was fully disabled and a Principal:* GetObject policy was applied to a restricted-classification bucket holding 18,442 customer export objects, making every object anonymously readable.

- `PutPublicAccessBlock` at 09:32:47Z set all four BPA flags (`BlockPublicAcls`, `IgnorePublicAcls`, `BlockPublicPolicy`, `RestrictPublicBuckets`) to false
- `PutBucketPolicy` at 09:34:12Z applied `Effect: Allow, Principal: *, Action: s3:GetObject` on the full object ARN - this is the alerting event
- The bucket is tagged `data-classification: restricted` and contains dated customer CSV exports produced by the former backup pipeline
- No legitimate public-hosting use case exists for this bucket; the CDN and website buckets live in a separate account
- Public exposure persisted 41 minutes until responders restored Block Public Access at 10:15:27Z and reverted the bucket policy at 10:16:02Z

▸ How we got the answer (2 data points)

Is this activity consistent with legitimate use of the svc-backup-legacy identity?

• Nothing about the identity's history explains this: the user was dormant for 63 days, has never called policy-modification APIs, holds an unrotated 311-day-old key with no MFA, and the retired pipeline it served only ever wrote objects from the VPC NAT range.

- IAM Access Advisor shows last activity 2026-05-07 (63 days prior); historical calls are exclusively `s3:PutObject` to a different backup bucket
- Zero prior `PutBucketPolicy`, `PutPublicAccessBlock`, or any `iam:*` / `s3:Put*Policy` calls by this principal in 365 days of CloudTrail
- The backup pipeline this user served was decommissioned in the 2026-05 cleanup (change record CHG-2214), but the IAM user and key were never removed
- The session began with `GetCallerIdentity` and `ListBuckets` - a recon pattern typical of a actor validating a found credential, not of automation
- No change ticket, deploy, or infrastructure-as-code run references this bucket or identity today; Terraform state shows no planned policy change

▸ How we got the answer (3 data points)

Where did the activity originate - operator tooling or attacker infrastructure?

• The calls came from first-seen datacenter infrastructure flagged by 21/93 threat-intel engines, with a user agent that does not match the identity's historical automation, indicating a stolen key used from attacker-controlled hosting.

- `198.51.100.77` belongs to ASN 64510 (Example Datacenter Corp), a hosting provider; `is_datacenter=true`, no corporate VPN or office egress association
- 21/93 VirusTotal engines flag the IP; GreyNoise classifies it as actively scanning cloud APIs over the past week
- First appearance of this IP and ASN anywhere in the account's 365-day CloudTrail history
- User agent `aws-cli/2.15.30` differs from the identity's historical `Boto3/1.26` automation signature
- No corporate device, VPN session, or SSO login correlates to the activity window for any employee associated with the legacy pipeline

▸ How we got the answer (2 data points)

Was data actually accessed during the exposure window, and what is the blast radius?

- **At least 3 anonymous GET requests from 2 external IPs are confirmed in server access logs, but CloudTrail data events were not enabled on the bucket, so the true read count during the 41-minute window is a lower bound and the object-level audit is still running.**

- S3 server access logs show 3 anonymous `REST.GET.OBJECT` requests between 09:41Z and 09:58Z from `203.0.113.150` and `203.0.113.161`, retrieving 2 distinct customer export objects
- CloudTrail S3 data events were not enabled for this bucket, so API-level read telemetry beyond access logs is unavailable for the window
- No `ListBucket` from anonymous principals appears in access logs, suggesting the readers used direct object URLs rather than enumeration
- No other buckets were modified and no IAM, EC2, or Lambda mutations were made by the key in the session; activity was scoped to this bucket
- The key made no further calls after 09:36Z; it was disabled by responders at 10:18:44Z

▸ How we got the answer (3 data points)

CONCLUSION

This is a confirmed malicious exposure of restricted customer data using a stolen long-lived credential. A 63-day-dormant IAM user with an unrotated, MFA-less access key performed credential-validation recon from flagged datacenter infrastructure, then stripped Block Public Access and published a `Principal: *` read policy on `example-corp-customer-exports`. Anonymous reads of at least 2 customer export objects are confirmed during the 41-minute window, and the absence of CloudTrail data events means the confirmed count is a floor, not a ceiling. Containment is done (key disabled, policy reverted, BPA restored); the remaining work is incident-grade: complete the object-access audit, treat the confirmed reads as a reportable data exposure per policy, hunt the credential-leak source since the key was used from infrastructure the pipeline never touched, and remove the standing-key attack surface that made this possible.

RECOMMENDED ACTIONS

MUST DO

1 HIGH **Confirm containment and delete the compromised credential path** - Access key `AKIAIOSFODNN7EXAMPLE` is disabled; now delete the key and the `svc-backup-legacy` IAM user entirely (pipeline retired in CHG-2214), and verify the bucket policy and all four Block Public Access settings match the pre-incident state.

2 HIGH **Complete the object-access audit and trigger data-incident handling** - Finish the Athena sweep of server access logs for the full window, identify the 2 retrieved objects and the customer records inside them, and hand off to privacy/legal for exposure assessment. Treat the confirmed anonymous reads as a reportable event pending their review.

3 HIGH **Hunt the credential-leak source** - The key was used from infrastructure the identity never touched. Run secret scanning across repos, CI logs, wiki, and ticket attachments for the key ID; review who had access to the retired pipeline's configuration; check paste-site and infostealer-marketplace monitoring for the key ID.

4 HIGH **Block the actor infrastructure and sweep for reuse** - Add 198.51.100.77 and the 2 anonymous-reader IPs to the account-level WAF/network denies where applicable, and sweep CloudTrail across all organization accounts for any activity from ASN 64510 in the past 90 days.

RECOMMENDED

5 MEDIUM **Enable CloudTrail S3 data events and GuardDuty S3 Protection for restricted buckets** - The read audit was limited to server access logs because data events were off. Enable data events for all buckets tagged restricted, and confirm GuardDuty S3 Protection is on in every production account.

6 MEDIUM **Apply an SCP guarding Block Public Access and public bucket policies** - Deny `s3:PutPublicAccessBlock` account-wide and `s3:PutBucketPolicy` containing wildcard principals except for an approved break-glass role, so a single stolen key can no longer publish a bucket.

7 MEDIUM **Retire dormant IAM users and enforce key hygiene** - Inventory IAM users with keys unused for 45+ days (this key sat dormant for 63), remove those tied to decommissioned systems, and enforce 90-day rotation with MFA or migration to short-lived role credentials.

▾ Attack Timeline

2026-07-09T09:31:12Z	GetCallerIdentity by svc-backup-legacy from 198.51.100.77 (first activity in 63 days; first-ever from this ASN) - credential validation
2026-07-09T09:31:40Z	ListBuckets enumerates 47 buckets in account 111122223333
2026-07-09T09:32:47Z	PutPublicAccessBlock disables all four Block Public Access settings on example-corp-customer-exports (T1562.007)
2026-07-09T09:34:12Z	PutBucketPolicy applies Principal:* s3:GetObject policy - alert triggered; GuardDuty Policy:S3 findings fire
2026-07-09T09:36:02Z	Final API calls by the key (3 failed GetBucketAcl attempts on unrelated buckets); no further activity
2026-07-09T09:41-09:58Z	3 anonymous GET requests from 203.0.113.150 and 203.0.113.161 retrieve 2 customer export objects (~14 MB) per server access logs
2026-07-09T10:15:27Z	Responders restore Block Public Access; bucket policy reverted at 10:16:02Z - exposure window closed (41 minutes)
2026-07-09T10:18:44Z	Access key AKIAIOSFODNN7EXAMPLE disabled; organization-wide ASN sweep initiated

▾ Indicators of Compromise

TYPE	INDICATOR	CONTEXT
IP	`198.51.100.77`	Actor API origin; ASN 64510 datacenter; 21/93 VT
IP	`203.0.113.150`, `203.0.113.161`	Anonymous object readers during exposure window
Access key	`AKIAIOSFODNN7EXAMPLE`	Compromised long-lived key (disabled 10:18:44Z)
IAM user	`svc-backup-legacy`	Dormant identity from retired pipeline (CHG-2214)
User agent	`aws-cli/2.15.30`	Actor tooling; identity historically used Boto3/1.26
Bucket	`example-corp-customer-exports`	Exposed restricted-classification customer data