INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:35 UTC

EU Executive Body Breached via Amazon Cloud Account: 350 GB Claimed Stolen, Leak Threatened

DATA BREACH | HIGH | CVSS 9.5

SCC Item ID	SCC-DBR-2026-0064
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Amazon Web Services cloud infrastructure (European Commission-managed account); European Commission email servers and employee data systems
Published	2026-03-27
Discovery Source	Rss

Executive Summary

A threat actor claims to have breached at least one AWS cloud account operated by or on behalf of the European Commission, exfiltrating a claimed 350 GB of data that includes email server content and employee databases. The attacker has publicly stated they will not seek ransom and intend to leak the data, a posture consistent with information operations or state-adjacent activity rather than financially motivated cybercrime. If confirmed, the breach represents a significant exposure of EU institutional communications and personnel data, with potential downstream risk to partner organizations and third parties whose data transits Commission systems.

Technical Analysis

The incident involves unauthorized access to an AWS cloud account associated with the European Commission, with claimed exfiltration of approximately 350 GB including email server data and employee records. Primary weakness indicators point to authentication failure (CWE-287: Improper Authentication) enabling cloud account compromise, with resulting sensitive data exposure (CWE-200). A possible Ivanti EPMM exploitation vector (CWE-94: Improper Control of Code Generation) has been inferred by some reporting based on authentication failure patterns observed in similar breaches; this inference has not been independently confirmed and should be treated as exploratory hypothesis, not confirmed attack vector. No CVE has been assigned to this incident as of reporting. MITRE ATT&CK techniques consistent with the described activity include: T1078 (Valid Accounts) and T1586 (Compromise Accounts) for initial access; T1190 (Exploit

Public-Facing Application) if the Ivanti vector is confirmed; T1114 (Email Collection) and T1530 (Data from Cloud Storage) for collection; T1537 (Transfer Data to Cloud Account) and T1567 (Exfiltration Over Web Service) for exfiltration. No patch status or vendor advisory is applicable to this incident in its current form, the attack vector appears to be credential or authentication-based cloud account compromise, not an unpatched software vulnerability. Source quality is moderate (T3 reporting only; no official Commission disclosure as of reporting date).

Action Checklist

1. Step 1: Containment, Audit all AWS IAM users, roles, and access keys for accounts with administrative or data-plane access to cloud storage, email integration, or employee data systems. Immediately rotate credentials for any account showing anomalous access patterns. If Ivanti EPMM is present in your environment, isolate or take offline until the low-confidence CWE-94 vector is ruled out. Reference: AWS IAM Access Analyzer and CloudTrail for access review.
2. Step 2: Detection, Query AWS CloudTrail for large-volume GetObject, CopyObject, or ListBucket events, particularly those accessing S3 buckets containing email or HR data. Look for API calls from unfamiliar IP ranges, unusual geographic locations, or service accounts not associated with known automation. Review IAM authentication logs for failed MFA challenges, token reuse anomalies, or successful logins following credential stuffing patterns. If Ivanti EPMM is deployed, check application logs for exploitation indicators. Note: prior Ivanti EPMM authentication bypass vulnerabilities (CVE-2023-35078, CVE-2023-35082) are referenced here as analogous attack patterns; current incident link to these CVEs is not confirmed.
3. Step 3: Eradication, Enforce MFA on all AWS IAM accounts, especially those with S3, SES, or WorkMail access. Revoke and reissue all long-lived access keys. Apply least-privilege IAM policies and remove any wildcard permissions. If Ivanti EPMM is confirmed as an initial access vector, apply all available patches from Ivanti's official security advisories and verify patch integrity. Remove unauthorized IAM roles or Lambda functions created during the compromise window.
4. Step 4: Recovery, Validate CloudTrail log integrity to confirm no tampering during the incident window. Re-enable services only after confirming credential rotation is complete and no persistence mechanisms (rogue IAM roles, Lambda backdoors, S3 event notifications pointing to attacker-controlled endpoints) remain. Enable AWS GuardDuty if not already active and review findings for the prior 90-day window. Notify affected personnel whose email or personal data may have been exposed, consistent with applicable GDPR breach notification obligations.
5. Step 5: Post-Incident, This incident exposes three recurring control gaps in cloud environments: over-privileged IAM identities, insufficient MFA enforcement, and inadequate monitoring of data-plane API activity. Map findings to NIST SP 800-53 controls AC-2 (Account Management), IA-5 (Authenticator Management), AU-12 (Audit Record Generation), and SI-4 (System Monitoring). Conduct a cloud security posture review against CIS AWS Foundations Benchmark. If state-adjacent or information operations activity is confirmed, brief leadership on potential follow-on targeting of partner organizations who share data with the Commission.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to CISO, legal counsel, and the European Data Protection Supervisor if CloudTrail or S3 access logs confirm any GetObject or CopyObject events against buckets containing employee PII or email content, as GDPR Article 33 requires notification to the supervisory authority within 72 hours of the organization becoming aware of a personal data breach, and the claimed 350 GB exfiltration including employee data systems meets the threshold for high-risk individual notification under Article 34; additionally escalate to national cybersecurity authority (e.g., CERT-EU or relevant Member State CSIRT) if state-adjacent or information operations attribution is supported by threat intelligence, given the potential for follow-on targeting of Commission partner organizations.
Recovery Notes	Re-enable AWS services in a staged sequence — begin with read-only service accounts verified against the pre-incident IAM baseline, then restore write-access roles only after a second-party review of the new least-privilege policy documents confirms no residual wildcard permissions. Monitor CloudTrail for recurrence of GetObject bulk activity and any new AssumeRole events for a minimum of 90 days post-recovery, as threat actors conducting information operations (leak-intent, no ransom) have a documented pattern of maintaining dormant secondary access for follow-on collection after initial discovery. Conduct a data impact assessment specific to the email server content and employee database exposure before issuing individual notifications under GDPR Article 34, as the scope and sensitivity of exposed data will determine both the notification obligation and the recommended protective actions for affected individuals.
Forensic Artifacts	AWS CloudTrail management and data-plane event logs (JSON, stored in the configured S3 logging bucket): specifically events GetObject, CopyObject, ListBucket, CreateAccessKey, AssumeRole, AttachUserPolicy, and PutBucketNotification — the data-plane events require S3 server access logging or CloudTrail S3 data event logging to be enabled separately from the default management event trail, and their absence is itself a forensic finding relevant to the 350 GB exfiltration scope determination | S3 server access logs for all buckets identified as containing email content or employee HR/PII data: these logs record individual object-level request byte counts and are the primary source for validating or refuting the claimed 350 GB exfiltration volume, as CloudTrail data events do not include response payload sizes | IAM credential report and Access Analyzer findings snapshot captured at the moment of detection: documents the full population of IAM users, roles, access key ages, MFA enrollment status, and cross-account trust relationships as a forensic baseline for identifying attacker-created identities and policy changes during the compromise window | Ivanti EPMM Tomcat access logs at `/opt/MobileIron/Tomcat/logs/access_log.*.txt`: if EPMM is present, these logs contain HTTP request records for the unauthenticated API endpoints `/mifs/aad/api/v2/admins/users` and `/api/v2/` that were exploited in CVE-2023-35078 (CVSS 10.0) and CVE-2023-35082, enabling reconstruction of the initial access timeline and identification of any attacker-controlled IP ranges used for pre-compromise reconnaissance | AWS Lambda function code packages and environment variables for all Lambda functions created or modified during the compromise window: attacker-deployed Lambda backdoors in cloud credential abuse campaigns commonly encode C2 callback URLs or exfiltration bucket ARNs in environment variables, and the function code itself may contain obfuscated scripts that clarify the attacker's data collection objectives and support attribution assessment relevant to the information operations hypothesis

Per-Action IR Details

Step 1: Containment — Audit all AWS IAM users, roles, and access keys for accounts with administrative or data-plane access to cloud storage, email integration, or employee data systems. Immediately rotate credentials for any account showing anomalous access patterns. If Ivanti EPMM is present in your

environment, isolate or take offline until the low-confidence CWE-94 vector is ruled out. Reference: AWS IAM Access Analyzer and CloudTrail for access review.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: short-term containment to stop ongoing damage while preserving evidence, with particular emphasis on isolating affected systems and revoking attacker-controlled credentials before evidence is destroyed

Controls: NIST AC-2 (Account Management) — audit and disable anomalous IAM identities, NIST IA-5 (Authenticator Management) — immediate rotation of compromised or suspect long-lived AWS access keys, NIST IR-4 (Incident Handling) — execute containment phase of incident handling capability, CIS 5.1 (Establish and Maintain an Inventory of Accounts) — enumerate all IAM users, roles, and service accounts before containment actions, CIS 6.2 (Establish an Access Revoking Process) — follow documented process for disabling or revoking access to AWS accounts showing anomalous activity

Compensating: Without AWS-native tooling budget: run `aws iam generate-credential-report && aws iam get-credential-report` via AWS CLI (free) to enumerate all IAM users and key ages. Pipe output through `jq` to filter for access keys unused >30 days or created during the suspected compromise window. For Ivanti EPMM isolation, implement an upstream firewall ACL blocking inbound TCP 443/8443 to the EPMM host from external IPs — a 2-person team can execute this in under 15 minutes without an EDR console.

Evidence: Before rotating any credentials, capture the full IAM credential report (`aws iam get-credential-report --output text --query Content | base64 -d`) to preserve key creation dates, last-used timestamps, and MFA enrollment status as a point-in-time forensic record. Pull all CloudTrail `AssumeRole`, `CreateAccessKey`, and `AttachUserPolicy` events for the prior 90 days before any IAM modifications — these event types document attacker persistence establishment in AWS and will be overwritten contextually once you begin remediation actions. If Ivanti EPMM is present, image the EPMM server's `/var/log/` directory and capture a running process list before isolation, as exploitation of CVE-2023-35078/35082 may leave web shell artifacts or reverse shell processes that isolation would interrupt but not preserve.

Step 2: Detection — Query AWS CloudTrail for large-volume GetObject, CopyObject, or ListBucket events, particularly those accessing S3 buckets containing email or HR data. Look for API calls from unfamiliar IP ranges, unusual geographic locations, or service accounts not associated with known automation. Review IAM authentication logs for failed MFA challenges, token reuse anomalies, or successful logins following credential stuffing patterns. If Ivanti EPMM is deployed, check application logs for exploitation indicators consistent with CVE-2023-35078 or CVE-2023-35082 (prior Ivanti EPMM authentication bypass vulnerabilities linked to CWE-287 and remote code execution).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to establish scope, timeline, and data accessed; the 350 GB exfiltration claim requires quantifying actual S3 data egress before scope can be defined

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — structured review of CloudTrail logs for data-plane exfiltration indicators, NIST AU-12 (Audit Record Generation) — verify CloudTrail was enabled and logging data-plane S3 events (not just management events) during the incident window, NIST SI-4 (System Monitoring) — analyze network and API-level indicators of large-volume object retrieval consistent with 350 GB exfiltration, NIST IR-5 (Incident Monitoring) — track and document all detected CloudTrail anomalies as incident artifacts, CIS 8.2 (Collect Audit Logs) — confirm audit logging was active and intact for CloudTrail, IAM, and S3 data-plane events before relying on absence of logs as evidence

Compensating: Without a SIEM: use AWS CloudTrail Lake or Athena (both have free tiers) to run SQL queries directly against CloudTrail logs. Query: `SELECT userIdentity.arn, sourceIPAddress, eventName, requestParameters, responseElements, eventTime FROM cloudtrail_logs WHERE eventName IN ('GetObject','CopyObject','ListBucket','GetBucketAcl') AND eventTime BETWEEN '2025-01-01' AND '2026-03-04' ORDER BY eventTime DESC`. For Ivanti EPMM, grep EPMM application logs at `/opt/MobileIron/Tomcat/logs/` for HTTP 200 responses to `/mifs/aad/api/v2/` endpoints (the unauthenticated API path exploited in CVE-2023-35078) from external IPs: `grep -E 'POST /mifs/aad/api/v2/|GET /mifs/aad/api/v2/' access_log* | grep -v '192.168\|10\.'`. For

credential stuffing detection, download IAM authentication events from CloudTrail and filter for `ConsoleLogin` events with `additionalEventData.MFAUsed = No` or `errorCode = Failed authentication`.

Evidence: Capture S3 server access logs (separate from CloudTrail — must be enabled per bucket; located at the configured S3 logging target bucket) for the buckets identified as containing email or HR data, as these logs record individual object-level GET/LIST requests with byte counts that can validate or refute the 350 GB exfiltration claim. Pull CloudTrail `CreateNetworkAclEntry`, `AuthorizeSecurityGroupIngress`, and `ModifyInstanceAttribute` events to detect attacker-created network paths for exfiltration channels. For Ivanti EPMM exploitation indicators, collect the Tomcat access log (`/opt/MobileIron/Tomcat/logs/access_log.YYYY-MM-DD.txt`) and search for anomalous POST requests to `/mifs/aad/api/v2/admins/users` or `/api/v2/` paths with non-internal source IPs, which are the specific API endpoints abused in CVE-2023-35078 unauthenticated access.

Step 3: Eradication — Enforce MFA on all AWS IAM accounts, especially those with S3, SES, or WorkMail access. Revoke and reissue all long-lived access keys. Apply least-privilege IAM policies and remove any wildcard permissions. If Ivanti EPMM is confirmed as an initial access vector, apply all available patches from Ivanti's official security advisories and verify patch integrity. Remove unauthorized IAM roles or Lambda functions created during the compromise window.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all attacker-established persistence mechanisms from the environment, including rogue IAM roles and Lambda backdoors, before recovery begins; eradication is not complete until every attacker-created identity and execution environment is confirmed removed

Controls: NIST IA-5 (Authenticator Management) — revoke and reissue all long-lived AWS access keys; enforce MFA for all IAM identities with S3, SES, or WorkMail permissions, NIST AC-6 (Least Privilege) — remove wildcard IAM policies (`Effect: Allow, Action: *, Resource: *`) and scope permissions to minimum required for each role or service account, NIST SI-2 (Flaw Remediation) — apply Ivanti EPMM patches from official Ivanti security advisories if EPMM is confirmed as the initial access vector, NIST CM-7 (Least Functionality) — disable or remove unauthorized Lambda functions and IAM roles created outside the change management process during the compromise window, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — audit and remove any IAM identities granted AdministratorAccess that are not documented administrative accounts, CIS 7.3 (Perform Automated Operating System Patch Management) — validate Ivanti EPMM patch version against Ivanti's published advisory hash or checksum before applying

Compensating: Without enterprise IAM tooling: use the AWS CLI to enumerate and delete unauthorized Lambda functions — `aws lambda list-functions --query 'Functions[*].[FunctionName,LastModified]'` filtered for functions created during the compromise window. To find wildcard IAM policies, run: `aws iam list-policies --scope Local | jq '.Policies[].PolicyName'` then `aws iam get-policy-version` on each to inspect documents for `Action: *` or `Resource: *`. For Ivanti EPMM patch verification, compare the installed RPM hash with Ivanti's published advisory checksum using `rpm -qa | grep -i mobileiron` and cross-reference against the patch version table in Ivanti Security Advisory PSIRT-2023-0010 (CVE-2023-35078) and PSIRT-2023-0011 (CVE-2023-35082).

Evidence: Before removing unauthorized IAM roles or Lambda functions, export the full policy document and trust relationship for each rogue identity (`aws iam get-role --role-name ` and `aws iam list-role-policies`), as these documents may reveal the attacker's intended persistence mechanism, privilege escalation path, or C2 callback configuration embedded in Lambda environment variables. Capture Lambda function code packages (`aws lambda get-function --function-name `) before deletion — attacker-deployed Lambda backdoors in AWS breaches commonly contain base64-encoded reverse shells or exfiltration scripts that constitute high-value forensic evidence for attribution. If Ivanti EPMM is in scope, collect a filesystem diff of the EPMM web application directory (`/opt/MobileIron/`) before patching, as web shells dropped via CVE-2023-35078 exploitation are typically placed in the Tomcat webapps directory.

Step 4: Recovery — Validate CloudTrail log integrity to confirm no tampering during the incident window. Re-enable services only after confirming credential rotation is complete and no persistence mechanisms (rogue IAM roles, Lambda backdoors, S3 event notifications pointing to attacker-controlled endpoints) remain. Enable AWS GuardDuty if not already active and review findings for the prior 90-day window. Notify affected personnel whose email or personal data may have been exposed, consistent with applicable GDPR

breach notification obligations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation only after verifying eradication is complete and monitoring is in place to detect recurrence; the 90-day GuardDuty retroactive review is a recovery-phase validation step to confirm no persistent access was established prior to the known incident window

Controls: NIST AU-9 (Protection of Audit Information) — validate CloudTrail log integrity via S3 object checksums and CloudTrail log file validation feature before relying on logs for recovery decisions, NIST IR-4 (Incident Handling) — execute recovery phase consistent with the incident response plan, including service restoration sequencing and validation checkpoints, NIST IR-6 (Incident Reporting) — notify affected personnel and relevant authorities per GDPR Article 33 (72-hour supervisory authority notification) and Article 34 (individual notification for high-risk exposure) obligations, NIST SI-4 (System Monitoring) — enable AWS GuardDuty and establish baseline monitoring before re-enabling production services to detect recurrence of credential abuse or data-plane exfiltration, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — verify no residual unpatched systems remain in the environment before restoring full service connectivity

Compensating: Without GuardDuty budget: deploy the open-source `cloud-custodian` tool (free, Python-based) with rules targeting S3 GetObject rate anomalies and IAM key usage from new geographic regions. Alternatively, enable CloudTrail log file validation (`aws cloudtrail update-trail --name --enable-log-file-validation`) — this is a native AWS feature with no additional cost that generates SHA-256 digest files for each log batch, allowing integrity verification with `aws cloudtrail validate-logs`. For GDPR breach notification tracking without a GRC platform, use the ENISA GDPR breach notification template (freely available at enisa.europa.eu) and document the 72-hour notification clock start from the confirmed detection timestamp.

Evidence: Before re-enabling any S3 bucket or email service, verify S3 event notification configurations (`aws s3api get-bucket-notification-configuration --bucket `) for all affected buckets — attackers targeting cloud environments for data operations commonly implant S3 event notifications that silently forward newly uploaded objects to attacker-controlled SQS queues or Lambda functions, creating persistent exfiltration channels that survive credential rotation. Validate CloudTrail log file integrity by running `aws cloudtrail validate-logs --trail-arn --start-time ` and reviewing for any `INVALID` digest entries, which would indicate attacker tampering with audit records during the breach window — a finding that would materially affect the accuracy of any GDPR breach scope assessment.

Step 5: Post-Incident — This incident exposes three recurring control gaps in cloud environments: over-privileged IAM identities, insufficient MFA enforcement, and inadequate monitoring of data-plane API activity. Map findings to NIST SP 800-53 controls AC-2 (Account Management), IA-5 (Authenticator Management), AU-12 (Audit Record Generation), and SI-4 (System Monitoring). Conduct a cloud security posture review against CIS AWS Foundations Benchmark. If state-adjacent or information operations activity is confirmed, brief leadership on potential follow-on targeting of partner organizations who share data with the Commission.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review to identify control gaps, update detection capabilities, and share threat intelligence; the information operations posture of this threat actor (no ransom, leak-intent) requires a follow-on threat briefing distinct from standard financially-motivated breach response

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to incorporate AWS-specific containment playbook steps validated during this incident, NIST AC-2 (Account Management) — remediate identified IAM over-privilege as a systemic finding, not just for accounts involved in this incident, NIST IA-5 (Authenticator Management) — enforce MFA organization-wide for all AWS IAM identities as a post-incident corrective action, NIST AU-12 (Audit Record Generation) — ensure S3 data-plane logging and CloudTrail are enabled for all accounts and regions, not just production accounts where monitoring was assumed active, NIST SI-4 (System Monitoring) — implement continuous monitoring of AWS data-plane API activity as a permanent control improvement, not a temporary incident response measure, NIST IR-8 (Incident Response Plan) — update the IR plan to include AWS-specific playbooks for cloud credential compromise and large-volume S3 exfiltration scenarios, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate cloud IAM posture review into the recurring vulnerability management cycle, CIS 7.2 (Establish and Maintain a Remediation Process) — document IAM

over-privilege and missing MFA as tracked remediation items with assigned owners and deadlines

Compensating: For the CIS AWS Foundations Benchmark posture review without a commercial CSPM: run `prowler` (free, open-source AWS security tool at github.com/prowler-cloud/prowler) with `prowler aws --compliance cis_aws_foundations_benchmark_v1.5` — it maps findings directly to CIS benchmark safeguards and generates a JSON report suitable for leadership briefing. For the threat intelligence sharing component related to potential state-adjacent activity, submit indicators (attacker IPs, IAM principal ARNs if attributable, exfiltration destination IPs) to MISP (free, self-hosted) or directly to ENISA's CERT-EU, which maintains intelligence-sharing relationships with EU member state CERTs relevant to European Commission partner organization notification.

Evidence: The post-incident lessons-learned review should include a formal comparison of the attacker's observed TTPs against MITRE ATT&CK Cloud matrix techniques T1530 (Data from Cloud Storage), T1078.004 (Valid Accounts: Cloud Accounts), and T1537 (Transfer Data to Cloud Account) to determine whether detection rules in place would have fired earlier — and document that gap analysis as evidence for control improvement prioritization. Preserve the complete CloudTrail event history for the incident window in immutable S3 storage (enable S3 Object Lock with Governance mode) before closing the incident, as GDPR Article 5(2) accountability obligations and potential regulatory investigation by the European Data Protection Supervisor may require production of this evidence months after the incident is closed.

Detection Guidance

Primary detection surface is AWS CloudTrail. Query for: (1) High-volume S3 data access events, GetObject or ListBucket calls exceeding baseline thresholds, especially against buckets tagged as containing PII, email, or HR data. (2) IAM authentication anomalies, console logins without MFA, successful logins from IPs not associated with known VPNs or office ranges, or access key usage outside normal hours. (3) Exfiltration indicators, PutObject calls to external S3 buckets (T1537) or outbound data transfers to web services not in your approved integration list (T1567). If Ivanti EPMM is present, review web server access logs for exploitation patterns associated with prior Ivanti authentication bypass CVEs, look for unauthenticated requests to API endpoints that should require credentials. Behavioral indicator: the attacker's stated intent to leak rather than ransom suggests data has already been staged or transferred; prioritize egress review over lateral movement hunting as the immediate detection focus. No confirmed IOCs are publicly available as of reporting date.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/european-commission-investigating-breach-after-amazon-cloud-hack/`	Primary T3 source reporting the incident — monitor for updates including official Commission disclosure or IOC release	LOW
URL	`https://www.techzine.eu/news/security/140026/european-commission-investigates-data-breach-in-amazon-cloud/`	Secondary T3 source corroborating the incident report	LOW

Framework Mappings

MITRE-ATTACK

- **T1537** — Transfer Data to Cloud Account
- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1114** — Email Collection
- **T1586** — Compromise Accounts
- **T1190** — Exploit Public-Facing Application
- **T1530** — Data from Cloud Storage

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **6.3**
- **6.4**
- **6.5**
- **16.10**

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.312(a)(1)** — Access Control

ISO-27001-2022

- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1537	Transfer Data to Cloud Account	Exfiltration
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1114	Email Collection	Collection
T1586	Compromise Accounts	Resource-Development
T1190	Exploit Public-Facing Application	Initial-Access
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
	https://www.bleepingcomputer.com/news/security/european-commission-...	T3
	https://www.bleepingcomputer.com/news/security/whole-foods-supplier...	T3
	https://www.bleepingcomputer.com/news/technology/cloudflare-hit-by-...	T3
European Commission investigates data breach in Amazon cloud	https://www.techzine.eu/news/security/140026/european-commission-in...	T3

Generated 2026-03-29 18:35 UTC by TJS Security Command Center