INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-08 14:47 UTC

Accenture Data Breach: Threat Actor Claims 35 GB Source Code and Credentials Theft

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0217
Type	Data Breach
Severity	HIGH
Affected Products	Accenture (internal systems, specific products/versions not disclosed)
Published	20 hours ago
Discovery Source	Serper

Executive Summary

A threat actor claims to have stolen approximately 35 GB of data from Accenture's internal systems, purportedly including source code and credentials, and has listed the data for sale. Accenture has confirmed it is investigating a security incident. If the claim is substantiated, the primary business risk is unauthorized access to proprietary intellectual property, potential exposure of client-related credentials or configurations, and downstream supply-chain risk to organizations that rely on Accenture for managed services or consulting engagements.

Technical Analysis

No CVE is associated with this incident. The breach claim is based on threat actor statements and secondary reporting; Accenture has confirmed investigation but has not released technical details or official breach confirmation as of the source publication date. Affected products, versions, and the initial access vector have not been disclosed by Accenture or confirmed by any authoritative first-party source. The threat actor's claim covers approximately 35 GB of data described as source code and credentials. MITRE ATT&CK techniques associated with the reported behavior are T1078 (Valid Accounts, suggesting possible credential-based initial access), T1567.002 (Exfiltration to Code Repository), and T1213 (Data from Information Repositories). Data authenticity and breach scope rest on threat actor claims and secondary reporting only; no CISA advisory, NVD entry, or official Accenture disclosure with technical specifics was present in the provided source set. Confidence in granular technical details is low.

Action Checklist

1. Containment, If your organization has an active Accenture managed-services engagement, audit shared credential stores, API keys, VPN tokens, and service accounts provisioned to or by Accenture personnel. Rotate any credentials that could have been accessible to third-party environments. Reference: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege).
2. Detection, Review authentication logs for anomalous access patterns on accounts associated with Accenture integrations or third-party service accounts. Query for logins from unexpected geographies, off-hours access, or bulk data-access events. Reference MITRE T1078 detection patterns: correlate successful authentications against known user baselines. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).
3. Eradication, Revoke and reissue all shared credentials, API tokens, and certificates provisioned to or managed in conjunction with Accenture where feasible. Enforce MFA on all externally exposed and administrative accounts as an immediate compensating control. Reference: NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), D3-CRO (Credential Rotation), D3-MFA (Multi-factor Authentication).
4. Recovery, After credential rotation, monitor for continued anomalous authentication attempts or unexpected data-access events. Validate that no persistent access mechanisms (scheduled tasks, implanted service accounts, or backdoor tokens) were established during the suspected access window. Reference: NIST SI-4 (System Monitoring), D3-LAM (Local Account Monitoring).
5. Post-Incident, Evaluate your third-party vendor risk management program for visibility into credential sharing, data co-mingling, and incident notification obligations with managed service providers. Conduct a privileged access audit across all third-party integrations. Reference: NIST AC-5 (Separation of Duties), NIST AC-20 (Use of External Systems), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if authentication log review confirms successful logins from Accenture-associated accounts after the breach disclosure date, if any rotated credential is found actively in use in production systems post-rotation, or if co-mingled data includes PII or PHI subject to GDPR Article 33, HIPAA Breach Notification Rule, or applicable state breach notification law (e.g., CCPA), as regulatory notification windows may already be running.
Recovery Notes	After completing credential rotation and eradication, maintain elevated monitoring on all formerly Accenture-integrated systems and identity planes for a minimum of 90 days, given the possibility that the threat actor retained exported credentials or source code that could enable delayed re-entry or supply-chain attacks against downstream clients. Specifically monitor for OAuth application consent events, new service principal registrations, and any CI/CD pipeline modifications that could represent delayed implant activation from code reviewed during the breach window. Verify integrity of any software artifacts (binaries, container images, packages) built from repositories that were potentially exposed, as the 35 GB source code theft creates a plausible supply-chain tampering vector for Accenture-delivered software.

Forensic Artifacts	Active Directory and LDAP audit logs: Windows Security Event IDs 4624, 4648, 4768, 4769, and 4776 on domain controllers — filter on Accenture-named or MSP-convention service accounts for the 90-day pre-disclosure window to identify the initial access timeframe and lateral movement via stolen credentials. | Source code repository access logs (GitHub Enterprise, GitLab, Bitbucket Server): focus on clone, archive-export, and bulk download events, particularly any single session transferring volumes consistent with the claimed 35 GB exfiltration — check for non-interactive or API-token-authenticated sessions performing repository enumeration. | Secrets management and credential vault audit logs (HashiCorp Vault, CyberArk PAS, Azure Key Vault diagnostic logs): secret read and list operations against paths accessible to Accenture service principals, especially bulk sequential reads that suggest automated credential harvesting rather than normal operational access. | Cloud identity platform audit logs (AWS CloudTrail `AssumeRole` and `GetFederationToken` events; Azure Entra ID Sign-in Logs and Audit Logs): cross-tenant federation activity, service principal password/certificate credential additions, and OAuth application consent grants during the breach window — persistent access via rogue app registration is a common post-credential-theft technique. | Network flow and proxy logs for data exfiltration fingerprinting: NetFlow or firewall session logs showing large outbound data transfers (targeting the approximate 35 GB volume) from systems hosting source code or credential stores, correlated against destination IPs and domains not in the organizational allowlist — particularly relevant if Accenture-managed VPN or remote access channels were used as the exfiltration path.

Per-Action IR Details

Containment — If your organization has an active Accenture managed-services engagement, audit shared credential stores, API keys, VPN tokens, and service accounts provisioned to or by Accenture personnel. Rotate any credentials that could have been accessible to third-party environments. Reference: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Without a PAM platform, enumerate service accounts using PowerShell: `Get-ADServiceAccount -Filter *` and cross-reference against accounts with 'Accenture', 'MSP', or contractor naming conventions. Export to CSV and flag any account with LastLogonDate within the suspected breach window. For API keys, grep application config directories and environment variable stores: `grep -rE '(api_key|token|secret)' /etc/app/ --include='*.conf' --include='*.env'`.

Evidence: BEFORE revoking any credential or token, capture: (1) Active directory authentication logs — Windows Security Event ID 4624 (successful logon) and 4648 (explicit credential use) for all service accounts tied to Accenture integrations, filtered for the 90-day window prior to breach disclosure; (2) VPN gateway session logs showing source IPs, session durations, and bytes transferred for Accenture-provisioned VPN accounts; (3) API gateway access logs showing all calls made under Accenture-managed API keys, particularly bulk GET or export-type requests against internal repositories or credential vaults; (4) Cloud IAM last-used timestamps for federated or cross-tenant service principal tokens before rotation invalidates the audit trail.

Detection — Review authentication logs for anomalous access patterns on accounts associated with Accenture integrations or third-party service accounts. Query for logins from unexpected geographies, off-hours access, or bulk data-access events. Reference MITRE T1078 detection patterns: correlate successful authentications against known user baselines. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell to query Windows Security Event logs directly on domain controllers: `Get-WinEvent -FilterHashtable @{LogName='Security'; Id=4624,4648,4768,4769} | Where-Object {$_.Message -match 'accenture|svc_msp|contractor'} | Export-Csv auth_review.csv`. For Linux-based systems hosting source code repositories (GitLab, Bitbucket), parse `/var/log/auth.log` and application access logs with `awk` or `grep` for off-hours timestamps and non-standard source IPs. Enrich IPs against free geo-lookup (ip-api.com) using a bash loop to flag non-expected countries.

Evidence: This step is analytical and does not alter live state; however, ensure log integrity is preserved before analysis: (1) Windows Security Event IDs 4624, 4648, 4768, 4769, and 4776 on domain controllers for all Accenture-associated accounts — this breach context implicates credential theft, so Kerberoasting artifacts (4769 with RC4 encryption type 0x17) are specifically relevant; (2) Source code repository access logs (GitHub Enterprise, GitLab, Bitbucket) for clone, archive-download, or bulk repository export events against internal repos — the 35 GB claim is consistent with bulk repository pulls; (3) Secrets management platform audit logs (HashiCorp Vault, CyberArk) for any secret read events on paths accessible to Accenture service principals; (4) Cloud trail logs (AWS CloudTrail, Azure Monitor) for cross-tenant federation token use or service principal activity originating from Accenture-managed tenants.

Eradication — Revoke and reissue all shared credentials, API tokens, and certificates provisioned to or managed in conjunction with Accenture where feasible. Enforce MFA on all externally exposed and administrative accounts as an immediate compensating control. Reference: NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), D3-CRO (Credential Rotation), D3-MFA (Multi-factor Authentication).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For teams without a PAM solution: generate new API keys and immediately update dependent application configs; use `openssl rand -hex 32` to create high-entropy replacement secrets. For certificate revocation, use your CA's CRL or OCSP endpoint — if internal PKI is managed by Accenture-adjacent infrastructure, treat all issued certs as potentially compromised and reissue from an isolated CA. For MFA enforcement without enterprise SSO, enable TOTP-based MFA on all VPN gateways (OpenVPN supports Google Authenticator via `openvpn-plugin-auth-pam`) and enforce it on any externally-facing admin panel (cPanel, Webmin, cloud console).

Evidence: BEFORE revoking certificates or rotating API credentials: (1) Capture full memory dump of any authentication proxy or secrets management server that Accenture personnel had access to — look for plaintext credential material in process heap associated with vault agents or credential broker processes; (2) Preserve the complete list of currently active sessions and issued tokens from OAuth/OIDC providers before invalidation — this snapshot is the only post-hoc evidence of what was active during the suspected breach window; (3) Export certificate transparency logs or internal CA issuance records for all certs issued to Accenture-managed entities; (4) Run `netstat -ano` or `ss -tulnp` on externally-facing systems to capture active connection state before any session termination actions are taken, preserving potential evidence of concurrent adversary sessions.

Recovery — After credential rotation, monitor for continued anomalous authentication attempts or unexpected data-access events. Validate that no persistent access mechanisms (scheduled tasks, implanted service accounts, or backdoor tokens) were established during the suspected access window. Reference: NIST SI-4 (System Monitoring), D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Without EDR, deploy Sysmon with a community config (SwiftOnSecurity or Olaf Hartong's modular config) to capture Event ID 1 (Process Create) and Event ID 13 (Registry modification) for persistence mechanisms. For scheduled task enumeration, run `schtasks /query /fo LIST /v > scheduled_tasks_baseline.txt` and diff against a pre-incident baseline if available. For implanted service accounts, compare current AD account inventory against the pre-breach snapshot using PowerShell: `Compare-Object (Import-Csv baseline_accounts.csv) (Get-ADUser -Filter * | Select SamAccountName,Enabled,Created)`. For backdoor OAuth tokens, audit all application registrations and service principal credentials in Azure AD / Entra ID via `Get-MgServicePrincipalPasswordCredential`.

Evidence: This step involves monitoring, not live-state alteration, but requires baseline snapshots BEFORE returning systems to production: (1) Full export of all scheduled tasks, startup items, WMI subscriptions, and service registrations on systems Accenture personnel had remote access to — persistence artifacts are the primary risk given the credential-theft nature of this breach; (2) Active Directory creation-date audit for any accounts created during the suspected breach window (`Get-ADUser -Filter {Created -ge '2024-01-01'} -Properties Created`); (3) OAuth application consent grants and delegated permission entries in cloud identity platforms — threat actors with stolen credentials commonly register rogue OAuth apps for persistent access; (4) Git repository commit history for any additions of backdoor code, hardcoded credentials, or CI/CD pipeline modifications during the breach window, given the 35 GB source code theft claim.

Post-Incident — Evaluate your third-party vendor risk management program for visibility into credential sharing, data co-mingling, and incident notification obligations with managed service providers. Conduct a privileged access audit across all third-party integrations. Reference: NIST AC-5 (Separation of Duties), NIST AC-20 (Use of External Systems), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-5 (Separation Of Duties), NIST AC-20 (Use Of External Systems), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without a GRC platform, conduct the privileged access audit using a structured spreadsheet: enumerate all third-party integrations, the accounts or API keys provisioned for each, the data or systems they can access, and the contractual notification SLA. Review your MSA or SOW with Accenture for breach notification clauses — most MSSP contracts require notification within 72 hours of confirmed breach, aligning with GDPR Article 33. For future credential isolation, implement Just-In-Time access using free tooling: HashiCorp Vault Community Edition supports dynamic secrets that auto-expire, eliminating shared long-lived credentials with MSP partners.

Evidence: Post-incident documentation should include: (1) Complete audit trail of all credential and token rotations performed during containment and eradication, with timestamps and responsible parties — required for regulatory notification packages; (2) Exported access logs for the full suspected breach window, preserved to immutable storage before log retention windows expire — AU-11 (Audit Record Retention) requires retention periods sufficient for after-the-fact investigations; (3) Contractual review artifacts: index of all Accenture-managed systems, data classifications of co-mingled data, and any data processing agreements that trigger breach notification obligations; (4) Lessons-learned documentation covering the gap between Accenture's incident and your organization's awareness, specifically quantifying detection latency as a program improvement metric per NIST 800-61r3 §4.

Detection Guidance

Focus detection on MITRE T1078 (Valid Accounts) and T1213 (Data from Information Repositories) behavioral indicators. Query identity and access management logs for: (1) service accounts or third-party accounts accessing large volumes of internal repositories or file shares in a compressed time window; (2) successful logins from IP ranges inconsistent with known Accenture or third-party egress points; (3) bulk download or archive creation events (T1567.002) on code repositories or document management systems. If your environment uses a SIEM, build detection rules correlating high-volume file-access events with accounts that

lack a routine baseline for that behavior. No confirmed IOCs were present in the provided source material; do not use unverified indicators in production detection rules. Reference: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis).

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1567.002** — Exfiltration to Cloud Storage
- **T1213** — Data from Information Repositories

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1567.002	Exfiltration to Cloud Storage	Exfiltration

Technique ID	Technique Name	Tactic
T1213	Data from Information Repositories	Collection

Sources

Source	URL	Tier
"35 GB of Accenture for Sale": Hacker claims source code ...	https://www.escudodigital.com/en/cybersecurity/35-gb-of-accenture-f...	T3

Generated 2026-07-08 14:47 UTC by TJS Security Command Center