INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:42 UTC

UK Companies House WebFiling Broken Access Control Exposed Five Million Company Records

DATA BREACH | **MEDIUM** | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0022
Type	Data Breach
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	Companies House WebFiling service (UK Government), all registered UK companies (~5 million), exposure window October 2025 through approximately March 2026
Published	2026-03-16

Executive Summary

A broken access control flaw in the UK Government's Companies House WebFiling service exposed private dashboard data for approximately five million registered UK companies between October 2025 and approximately March 2026. Any authenticated user could access another company's filing dashboard, including director home addresses, dates of birth, and email addresses, by pressing the browser back button after a failed login. The exposure window of roughly five months, combined with the trivial exploitation method, creates material risk of identity fraud, targeted phishing against directors, and potentially fraudulent company filings.

Technical Analysis

The vulnerability resided in the Companies House WebFiling authentication and session management layer. After a failed authentication attempt, pressing the browser back button bypassed session validation and dropped an authenticated user into another company's private dashboard without re-authorization. No exploit tooling, scripting, or elevated access was required. Root cause maps to CWE-284 (Improper Access Control), CWE-285 (Improper Authorization), CWE-306 (Missing Authentication for Critical Function), and CWE-613 (Insufficient Session Expiration), the application failed to invalidate or re-validate session state on navigation, allowing cross-account access via browser history traversal. MITRE ATT&CK techniques include T1078 (Valid Accounts, authenticated entry point required), T1087 (Account Discovery, directory-level enumeration possible), and T1565.001 (Stored Data Manipulation, unauthorized filings potentially possible). No CVE has been assigned. CVSS 5.0 is an analyst estimate based on CWE severity; no vendor CVSS has been published and should not be relied upon as the primary severity indicator for a five-million-record exposure. Remediation was applied approximately March 2026; Companies House has confirmed the flaw. Sources: BleepingComputer (https://ww

w.bleepingcomputer.com/news/security/uks-companies-house-confirms-security-flaw-exposed-business-data/) and Tax Policy Associates (https://taxpolicy.org.uk/2026/03/13/companies-house-security-vulnerability-directors-addresses/), both T3 sources; treat as unconfirmed pending official Companies House advisory.

Action Checklist

1. Step 1, Verify remediation status: Confirm with Companies House directly that the access control fix is fully deployed and no residual exposure exists before resuming normal filing operations.
2. Step 2, Assess director data exposure: Identify all directors and persons of significant control (PSCs) associated with your registered UK companies. Determine what personal data, home addresses, dates of birth, email addresses, was held in WebFiling and treat it as compromised for the October 2025 to March 2026 window.
3. Step 3, Review your company filings for tampering: Log into WebFiling and audit all filings submitted during the exposure window. Flag any unauthorized submissions to Companies House and request correction under the Companies Act 2006 process.
4. Step 4, Notify affected individuals: Under UK GDPR, assess whether the exposure of director personal data constitutes a reportable breach to the ICO. If the threshold is met, notify affected directors and submit to the ICO within 72 hours of discovery. Consult your DPO or legal counsel for this determination.
5. Step 5, Harden third-party access dependencies: Review all systems and processes that rely on Companies House data as an authoritative source, KYC workflows, credit checks, onboarding pipelines. Treat any director or company data sourced from Companies House during the exposure window as potentially tampered or unreliable and re-verify through an alternative source where decision-critical.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership and board/governance immediately if director exposure affects 50+ individuals; escalate to external IR/breach counsel and UK legal representation if ICO notification threshold is met or if internal re-verification reveals evidence of unauthorized filing submissions.
Recovery Notes	Post-breach recovery requires three parallel workstreams: (1) Legal/Compliance — ICO notification and GDPR documentation (72-hour window is binding); (2) Operational — re-verification of all KYC and decision-critical workflows that consumed Companies House data during the breach window, with secondary verification sources, to restore confidence in downstream systems; (3) Monitoring — implement continuous monitoring of your Companies House WebFiling account for unauthorized access attempts (log all logins and export activity for 12 months post-breach) and set alerts for any anomalous filing submissions or dashboard access patterns. Document all remediation steps in a lessons-learned report tied to NIST 800-61r3 §4.3.

Forensic Artifacts	Companies House WebFiling account access logs (login timestamps, user IDs, IP addresses, actions taken) — request from Companies House or your account audit trail | Browser history and HTTP session artifacts (cookies, tokens, Referer headers) from any account that accessed WebFiling during 2025-10-01 to 2026-03-31 | Internal audit logs from any system that consumed Companies House API data (query logs, API response payloads, timestamps of data import) | Email and messaging history referencing Companies House breach discovery (Slack, internal email with timestamps and discovery date) | Database transaction logs from all systems that stored or processed Companies House director/company data (before-after snapshots for 2025-10-01 to 2026-03-31 window)

Per-Action IR Details

Step 1, Verify remediation status: Confirm with Companies House directly that the access control fix is fully deployed and no residual exposure exists before resuming normal filing operations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4.2 (Recovery) — verification of remediation before resumption of service

Controls: NIST SI-2 (Flaw Remediation), NIST CA-7 (Continuous Monitoring), CIS 2.3 (Address Unauthorized Software)

Compensating: Request written confirmation from Companies House that includes: (1) timestamp of fix deployment, (2) list of access control tests executed post-fix, (3) confirmation no back-button exploitation is possible. Document all correspondence in an audit log with date/time stamps. If written confirmation is unavailable, conduct independent verification: attempt back-button exploitation on a test account; capture HTTP response headers and session tokens to confirm access is denied; screenshot the result with timestamp.

Evidence: Before contacting Companies House: (1) capture current WebFiling session tokens and authentication cookies (browser DevTools > Application > Cookies), (2) document current fix deployment date from Companies House status page with screenshot, (3) preserve any internal communication threads that reference the breach timeline or remediation window.

Step 2, Assess director data exposure: Identify all directors and persons of significant control (PSCs) associated with your registered UK companies. Determine what personal data, home addresses, dates of birth, email addresses, was held in WebFiling and treat it as compromised for the October 2025 to March 2026 window.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Analysis — scope determination) and NIST 800-53 AU-2 (Audit Events)

Controls: NIST IR-4(1) (Incident Handling — Incident Detection Procedures), NIST SA-3 (System Development Life Cycle), CIS 1.1 (Inventory of Authorized Assets)

Compensating: Without an enterprise data discovery tool: (1) export director/PSC records from your Companies House filing portal (File > Export) and save to a secure location with write-protect enabled, (2) cross-reference each director against your internal HR/payroll system to confirm data fields held (address, DOB, email), (3) create a spreadsheet listing: Company Registration Number | Director Name | Data Fields Held | Date Added to WebFiling | Date Removed (if applicable). Mark all entries with submission dates between 2025-10-01 and 2026-03-31 as 'exposed'. Share only with authorized personnel (legal, DPO, leadership) via encrypted email.

Evidence: Before conducting assessment: (1) preserve a read-only copy of your current Companies House filing records (screenshot or export with timestamp), (2) capture any internal communication referencing director data held in WebFiling, (3) preserve audit logs from your WebFiling account showing who accessed the filing dashboard and when (if available via Companies House account history).

Step 3, Review your company filings for tampering: Log into WebFiling and audit all filings submitted during the exposure window. Flag any unauthorized submissions to Companies House and request correction under the Companies Act 2006 process.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.4 (Analysis — evidence examination) and NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST IR-4(2) (Incident Handling — Dynamic Reconfiguration), NIST AU-6 (Audit Review, Analysis, and Reporting), CIS 3.14 (Log Review, Compliance Checks, and Summaries)

Compensating: Manually audit without automated diffing: (1) download a complete export of all filings from your WebFiling account for October 2025–March 2026, (2) compare each filing against your internal company records (board minutes, director updates, statutory filings) to identify discrepancies in submission dates, document versions, signer names, (3) for any mismatch, document: filing reference number, original submission date per your records, metadata per WebFiling, discrepancy description. (4) Contact Companies House Filing Support and submit a statutory notice of error under Companies Act 2006 §454 with evidence of the discrepancy; preserve the response in your audit trail.

Evidence: Before reviewing filings: (1) take a full-page screenshot of your WebFiling dashboard home page (with submission date range visible) and save with timestamp, (2) export the complete filing history report (if available) with submission times and user IDs, (3) preserve your internal master copy of submitted documents (Word, PDF, email confirmations) dated before the exposure window, (4) capture browser HTTP traffic during your WebFiling session review (use a network capture tool like Wireshark or browser DevTools Network tab) to detect any unauthorized API calls or data access.

Step 4, Notify affected individuals: Under UK GDPR, assess whether the exposure of director personal data constitutes a reportable breach to the ICO. If the threshold is met, notify affected directors and submit to the ICO within 72 hours of discovery. Consult your DPO or legal counsel for this determination.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment) and NIST 800-53 IR-6 (Incident Reporting)

Controls: NIST IR-4(4) (Incident Handling — Information Spillage Response), NIST SA-12 (Supply Chain Protection), CIS 6.5 (Access Control Testing)

Compensating: DPO or legal counsel is required for this step — do not attempt a GDPR breach assessment without qualified counsel. However, to prepare: (1) document all facts before contacting counsel: date of discovery, number of individuals affected, data types exposed, exploit window duration, evidence that unauthorized access occurred (exploitation proof); (2) preserve all communications with Companies House regarding the breach in a timestamped folder; (3) create a notification template listing director name, company name, data types exposed (DOB, address, email), exposure dates, mitigation steps, and contact information for questions — run this by counsel before sending.

Evidence: Before notifying: (1) capture Companies House public status page announcing the breach (screenshot with URL and timestamp), (2) preserve the date/time you discovered the breach (email to self, Slack message, or incident ticket timestamp), (3) document all directors/PSCs affected with their contact information, (4) preserve a copy of any internal risk assessment or data impact analysis prepared for counsel.

Step 5, Harden third-party access dependencies: Review all systems and processes that rely on Companies House data as an authoritative source, KYC workflows, credit checks, onboarding pipelines. Treat any director or company data sourced from Companies House during the exposure window as potentially tampered or unreliable and re-verify through an alternative source where decision-critical.

NIST Phase: Recovery

Reference: NIST 800-61r3 §4.3 (Post-Incident Activities — Lessons Learned) and NIST 800-53 SI-7 (Information System Monitoring)

Controls: NIST CA-7 (Continuous Monitoring), NIST SA-3(1) (System Development Life Cycle — Security Requirements), CIS 2.1 (Address Unauthorized Hardware)

Compensating: Without enterprise API monitoring: (1) audit all outbound integrations to Companies House: grep your code repositories and integration configs for Companies House API endpoints and data imports; list all systems that consume Companies House director/company data, (2) for each system, identify the use case (KYC, credit checks, onboarding) and data freshness requirement, (3) for decision-critical workflows (account approval, credit decisions), implement manual re-verification: require a second data source (e.g., credit bureau, government-issued ID check, or

direct director contact) before approving accounts if director data was sourced from Companies House between 2025-10-01 and 2026-03-31; document the re-verification step in your procedure, (4) for non-critical workflows, flag the data as 'unverified during breach window' in your database and set a review date after the breach is fully investigated.

Evidence: Before hardening: (1) capture a network flow diagram showing all integrations with Companies House (Visio, draw.io, or ASCII diagram with timestamp), (2) preserve API logs from your integration layer showing all Companies House API calls made between 2025-10-01 and 2026-03-31 (if available), (3) document the data fields imported from each API call, (4) preserve any alerts or monitoring thresholds you have on data freshness or anomalies during the exposure window.

Detection Guidance

Direct detection within your own environment is limited, this was a server-side access control flaw on a UK government platform, not malware or network intrusion. Focus detection effort on downstream indicators: (1) Monitor for phishing attempts targeting directors whose home addresses or emails were registered in WebFiling; the exposed data set is high-value for spear-phishing and fraud. (2) Review email logs and mail gateways for inbound messages referencing Companies House, director registration, or filing notifications sent to director email addresses during October 2025 through March 2026, these may indicate adversarial use of harvested contact data. (3) If your organization uses Companies House data in automated pipelines, check data integrity logs for unexpected changes to company records during the exposure window. (4) No IOCs (IPs, domains, hashes) have been published in connection with this vulnerability; exploitation was passive browser-based access requiring no external infrastructure. (5) Tax Policy Associates' analysis (https://taxpolicy.org.uk/2026/03/13/companies-house-security-vulnerability-directors-addresses/) provides additional technical context useful for understanding the scope of data accessible.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1565** — Data Manipulation
- **T1530** — Data from Cloud Storage
- **T1550** — Use Alternate Authentication Material
- **T1087** — Account Discovery
- **T1565.001** — Stored Data Manipulation

OWASP-TOP10-2021

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

NIST-800-53R5

- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)

CIS-V8

- **6.1**

- **6.2**
- **6.3**

SOC2-TSC

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

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1565	Data Manipulation	Impact
T1530	Data from Cloud Storage	Collection
T1550	Use Alternate Authentication Material	Defense-Evasion
T1087	Account Discovery	Discovery
T1565.001	Stored Data Manipulation	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/uks-companies-house-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/uks-companies-house-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/over-266-000-f5-big-...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/massive-allianz-life...	T3
Companies House vulnerability enabled company hijacking	https://taxpolicy.org.uk/2026/03/13/companies-house-security-vulner...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:42 UTC by TJS Security Command Center