INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

UK Government Registry Exposed Five Million Companies’ Private Data for Five Months via Logic Flaw

DATA BREACH | MEDIUM | CVSS 5.0

SCC Item ID	SCC-DBR-2026-0024
Type	Data Breach
Severity	MEDIUM
CVSS Base Score	5.0
Affected Products	UK Companies House WebFiling service (October 2025 - March 2026)
Published	2026-03-16

Executive Summary

A broken access control flaw in the UK Companies House WebFiling service exposed private records for approximately five million registered companies for five months, from October 2025 through March 2026. Any authenticated user could access or modify records belonging to other companies using only a valid login and a target company's registration number. Exposed data included home addresses, dates of birth, and email addresses of company officers and directors, information that directly enables identity fraud, targeted phishing, and social engineering against UK business leadership.

Technical Analysis

The vulnerability is an Insecure Direct Object Reference (IDOR) affecting the UK Companies House WebFiling service, classified under CWE-639 (Authorization Bypass Through User-Controlled Key) and CWE-284 (Improper Access Control). No CVE has been assigned. The official GOV.UK advisory confirms the flaw and its remediation. Attack complexity was low: exploitation required only a valid WebFiling account and enumeration of company registration numbers, which are publicly available. No elevated privileges, specialized tooling, or chained vulnerabilities were required. Exposed data fields include officer/director home addresses, dates of birth, and company email addresses. The flaw was active for approximately five months before being patched. The assigned CVSS base score of 5.0 (Medium) is assessed as potentially understated given the breadth of exposure (approximately five million companies), low attack complexity, and sensitivity of PII involved. No EPSS score or KEV listing is available. Relevant MITRE ATT&CK techniques include T1190 (Exploit Public-Facing Application), T1213 (Data from Information Repositories), T1087 (Account Discovery), T1078 (Valid Accounts), and T1565 (Data Manipulation). No confirmed threat actor attribution.

Action Checklist

1. Step 1, Verify patch status: Confirm the WebFiling service patch has been applied by checking the GOV.UK advisory at https://www.gov.uk/government/news/update-on-companies-house-webfiling-security-issue. If your organization operates or integrates with WebFiling, confirm the patched version is in production.
2. Step 2, Assess data exposure window: Determine whether your organization's registered companies, officers, or directors have active filings on Companies House WebFiling. Any UK-registered entity with records on the service during October 2025 to March 2026 should be treated as potentially exposed.
3. Step 3, Review access logs for anomalous record queries: If your organization has any direct access to WebFiling, audit logs for the October 2025 to March 2026 window for unauthorized or anomalous record access patterns, particularly bulk enumeration of company registration numbers or access to records not associated with your registered entity.
4. Step 4, Notify affected individuals: If officer or director PII (home addresses, dates of birth) was potentially exposed, notify those individuals per applicable data protection obligations under UK GDPR. Assess whether a reportable breach notification to the ICO is required.
5. Step 5, Harden IDOR controls in your own applications: Use this incident as a trigger to audit your own web applications for IDOR vulnerabilities. Verify that object-level authorization checks are enforced server-side and do not rely solely on user-supplied identifiers. Reference OWASP API Security Top 10: API1 (Broken Object Level Authorization) for remediation guidance.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to management and external IR firm immediately if internal audit reveals unauthorized access to your organization's data during Oct 2025–Mar 2026, or if affected officers/directors report suspicious activity (identity theft, phishing, credential abuse) following exposure notification.
Recovery Notes	Post-containment, conduct a 30-day monitoring period for affected officers/directors: monitor credit reports, phishing campaign volumes, and dark web credential markets for exposed email/phone numbers. Implement multi-factor authentication (MFA) for all WebFiling accounts and sensitive internal applications to mitigate credential-based attacks on exposed identities. Schedule a post-incident review 2 weeks post-closure to document lessons learned on IDOR detection, breach notification workflows, and access control testing maturity.
Forensic Artifacts	Companies House register export (company numbers, filing dates, officer/director names and addresses for Oct 2025–Mar 2026 period) | WebFiling HTTP access logs and proxy logs (source IP, authenticated user, target company numbers, timestamps) | Browser history and cache for all users with WebFiling access (Chrome History DB, Firefox places.sqlite, Safari History.db) | Internal HR/corporate records linking officers/directors to company registrations (board minutes, entity ownership documentation, employment records) | Application authentication logs and session records (token generation, user login timestamps, IP addresses associated with WebFiling access)

Per-Action IR Details

Step 1, Verify patch status: Confirm the WebFiling service patch has been applied by checking the GOV.UK advisory at https://www.gov.uk/government/news/update-on-companies-house-webfiling-security-issue. If your organization operates or integrates with WebFiling, confirm the patched version is in production.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools, techniques, and procedures)

Controls: NIST 800-53 SI-2 (Flaw Remediation), NIST 800-53 CM-3 (Configuration Change Control), CIS 2.1 (Address Unauthorized Software), CIS 7.2 (Ensure Software is Supported by Vendor)

Compensating: If you lack automated patch management, create a manual verification checklist: (1) Log into WebFiling as an authenticated test user; (2) Verify the application footer or administration panel displays the patched version number matching GOV.UK advisory (post-March 2026 build); (3) Document the verification date and tester identity in a spreadsheet for audit trail. Cross-reference against the official advisory release date to confirm production deployment lag.

Evidence: Capture application version strings before and after patch application (screenshot of WebFiling admin panel, API response headers listing version). If integrated via API, log HTTP response headers (Server, X-Application-Version) from a test request dated post-patch. Preserve any system change logs, deployment tickets, or configuration management records showing patch deployment timestamp and personnel.

Step 2, Assess data exposure window: Determine whether your organization's registered companies, officers, or directors have active filings on Companies House WebFiling. Any UK-registered entity with records on the service during October 2025 to March 2026 should be treated as potentially exposed.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1 (Detection and Analysis: scope determination)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 CA-7 (Continuous Monitoring), CIS 6.2 (Address Unauthorized Software), CIS 8.5 (Account Monitoring and Control)

Compensating: Query Companies House freely available register at https://beta.companieshouse.gov.uk/ for each entity your organization owns or operates (use entity name or company number). If results show filings dated between October 2025–March 2026, that entity is exposed. For officers/directors, cross-reference internal HR records against filed officer names and addresses. Document the exposure scope in a spreadsheet (entity name, company number, filing dates in exposure window, PII categories). No special tools required—only web browser and internal records access.

Evidence: Screenshot or export the Companies House register entries for each affected entity (timestamp, filing dates, officer/director names visible). Preserve internal corporate records linking officers/directors to filings (HR records, board minutes, entity ownership documentation). Document the date you performed this assessment for timeline credibility.

Step 3, Review access logs for anomalous record queries: If your organization has any direct access to WebFiling, audit logs for the October 2025 to March 2026 window for unauthorized or anomalous record access patterns, particularly bulk enumeration of company registration numbers or access to records not associated with your registered entity.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (Perform event data analysis and investigation)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), NIST 800-53 AC-2 (Account Management), CIS 8.2 (Configure Data Access Control Measures)

Compensating: If WebFiling is accessed via web browser only: Export browser history for all users during Oct 2025–Mar 2026 using browser sync/export tools (Chrome: Sync data, Firefox: History export). Search for WebFiling URLs with non-standard query parameters (e.g., company numbers not matching your entities, bulk enumeration patterns in URL sequences). Filter access logs by timestamp, user account, and target company registration numbers. Create a manual log: user, access date/time, company number accessed, outcome. If accessed via API or integration: Request raw HTTP request/response logs from your application gateway or proxy (if available) for the exposure window; search for GET requests to WebFiling API endpoints with company numbers outside your registered entity list.

Grep command example: `grep -i 'webfiling.*company.*[0-9]{8}' /var/log/proxy.log | grep -v 'YOUR_COMPANY_NUMBERS' > suspicious_access.txt`.

Evidence: Export browser history/cache for all organizational accounts with WebFiling access (Chrome History file: `~/.config/google-chrome/Default/History`; Firefox: `~/.mozilla/firefox/*/places.sqlite`). Preserve proxy/firewall logs covering Oct 2025–Mar 2026 (netflow, WAF logs, HTTP access logs with full URL and user-agent). If WebFiling integration exists, capture application logs showing authentication tokens, request headers, and target entity identifiers. Document any gaps in log retention (e.g., logs older than X days were purged) to establish investigation scope limits.

Step 4, Notify affected individuals: If officer or director PII (home addresses, dates of birth) was potentially exposed, notify those individuals per applicable data protection obligations under UK GDPR. Assess whether a reportable breach notification to the ICO is required.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment, Eradication, and Recovery)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IA-4 (Identifier Management), CIS 6.5 (Require MFA), CIS 8.1 (Establish and Maintain a Data Classification Scheme)

Compensating: Create a breach notification checklist: (1) Confirm PII exposure eligibility with legal/compliance (does your organization have direct controller responsibility for the exposed data, or is exposure second-hand via Companies House?); (2) If controller, compile affected individual contact list from internal HR/corporate records for each exposed officer/director; (3) Draft notification template per UK GDPR Article 34 (include: what data, when exposed, steps taken, contact for questions); (4) Send via secure channel (registered mail or secure email) to each individual's last known address; (5) Document each notification sent (recipient, date, method, confirmation of delivery); (6) Submit breach report to ICO at https://ico.org.uk/make-a-complaint/ if exposure meets threshold (substantial risk to rights/freedoms). Use free templates from ICO guidance (https://ico.org.uk/for-organisations/data-protection/data-breaches/).

Evidence: Preserve the breach notification decision log (date decision made, personnel involved, reasoning for controller status). Retain copies of all notifications sent (email headers, postal receipts, delivery confirmations). Document ICO report submission confirmation (reference number, timestamp). Maintain a breach register entry per UK GDPR Article 33(5).

Step 5, Harden IDOR controls in your own applications: Use this incident as a trigger to audit your own web applications for IDOR vulnerabilities. Verify that object-level authorization checks are enforced server-side and do not rely solely on user-supplied identifiers. Reference OWASP API Security Top 10: API1 (Broken Object Level Authorization) for remediation guidance.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities)

Controls: NIST 800-53 AC-3 (Access Enforcement), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), CIS 3.3 (Address Unauthorized Software), CIS 14.9 (Implement and Manage a Secure Software Development Process)

Compensating: Conduct manual IDOR audit: (1) For each user-facing resource in your application (account, order, document, record), identify the unique identifier (ID, primary key, account number); (2) Log in as User A, access a legitimate resource (note the URL/API endpoint and ID); (3) Modify the ID parameter to a value belonging to User B; (4) If User B's data is returned without error, IDOR exists; (5) For each vulnerability: add server-side access control logic—before returning data, verify the authenticated user's authorization using session context or role-based rules, not user-supplied IDs; (6) Test remediation by repeating steps 2–4 to confirm User A cannot access User B's data. Use free tools: Burp Suite Community (manual request editing), OWASP ZAP (automated scanning), or browser dev tools (F12) to intercept and modify requests. Document findings in a spreadsheet (endpoint, vulnerability type, severity, remediation, re-test result).

Evidence: Capture proof-of-concept requests/responses showing IDOR vulnerability (HTTP request with modified ID parameter, response showing unauthorized data). Before-and-after code diffs showing authorization checks added to vulnerable endpoints. Re-test results confirming remediation (screenshots or logs showing access denied when unauthorized ID is supplied). Include developers involved and code review documentation.

Detection Guidance

Direct detection applies only if your organization operates, integrates with, or has built systems on top of the Companies House WebFiling service. For those environments, review server-side access logs for the October 2025 to March 2026 window and look for: (1) authenticated sessions accessing company records at an abnormal rate or volume, particularly sequential or incremental company registration number patterns suggesting enumeration; (2) access to records belonging to companies not associated with the authenticated account's registered entity; (3) any write or modification events on records outside normal business hours or from unexpected IP ranges. For organizations assessing indirect exposure, there are no network-level IOCs tied to this incident. The primary indicator of exploitation is the data itself appearing in phishing lures, social engineering attempts, or fraud targeting your company officers and directors. Monitor for spear-phishing campaigns using officer home addresses or personal details that would not be available through normal public sources. No confirmed IOCs have been published.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1213** — Data from Information Repositories
- **T1565** — Data Manipulation
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage
- **T1213** — Data from Information Repositories
- **T1087** — Account Discovery

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1**
- **6.2**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1213	Data from Information Repositories	Collection
T1565	Data Manipulation	Impact
T1530	Data from Cloud Storage	Collection
T1087	Account Discovery	Discovery

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/ibm-warns-of-critica...	T3
BleepingComputer	https://www.bleepingcomputer.com/news/security/over-266-000-f5-big-...	T3
Update on Companies House WebFiling security issue - GOV.UK	https://www.gov.uk/government/news/update-on-companies-house-webfil...	T1

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