INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-14 13:36 UTC

Iranian Cyber Group Handala Claims Breach of California Water Utility Billing Systems

DATA BREACH | **HIGH** | CVSS 8.1

SCC Item ID	SCC-DBR-2026-0172
Type	Data Breach
Severity	HIGH
CVSS Base Score	8.1
Affected Products	California Water Service Company (Cal Water), customer billing systems, RTKBase GNSS platform
Published	2026-06-14
Discovery Source	Gemini

Executive Summary

Iran-linked hacktivist group Handala claims to have breached California Water Service Company (Cal Water), allegedly exfiltrating approximately 5 GB of data from customer billing systems and an RTKBase GNSS geospatial platform. If confirmed, the breach exposes customer PII and financial data affecting one of the largest publicly traded water utilities in the United States, with secondary exposure of geospatial infrastructure data. Attribution and exfiltration volume remain unverified by Cal Water or CISA; no operational technology disruption has been independently confirmed.

Technical Analysis

Handala, an Iran-linked hacktivist/threat actor group, claims unauthorized access to Cal Water customer billing systems and an RTKBase GNSS base station platform. The alleged exfiltration totals approximately 5 GB. RTKBase is an open-source GNSS positioning software; its presence in a water utility environment suggests integration with field survey or infrastructure mapping workflows, representing an unusual geospatial data exposure vector alongside conventional billing PII. Relevant CWEs: CWE-522 (Insufficiently Protected Credentials), CWE-284 (Improper Access Control), CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor). MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1078 (Valid Accounts), T1566 (Phishing), T1213 (Data from Information Repositories), T1530 (Data from Cloud Storage), T1567 (Exfiltration Over Web Service). No CVE has been assigned. No Cal Water official disclosure or CISA advisory has been published as of the configuration date. Source quality is moderate (score 0.64); all sources are Tier 3, including Dataminr Intel Brief and Reddit/pwnhub community reporting. Independent verification of the 5 GB claim is pending.

Action Checklist

1. Containment: Audit and restrict external access to billing system interfaces and any internet-exposed RTKBase GNSS instances; enforce NIST AC-17 (Remote Access) by reviewing and tightening remote access policies; apply CIS 4.4 and CIS 4.5 to verify firewall rules block unauthenticated access to billing and geospatial platforms.
2. Detection: Review authentication logs on billing system and RTKBase hosts for anomalous logins, large data transfers, or access from Iranian IP ranges; apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) to search for T1078 (Valid Accounts) and T1567 (Exfiltration Over Web Service) indicators; enable D3-LAM (Local Account Monitoring) to surface unauthorized local account activity; query for bulk SELECT queries or export events against billing database tables in the relevant timeframe.
3. Eradication: Rotate all credentials associated with billing system service accounts and RTKBase platform per D3-CRO (Credential Rotation) and D3-CH (Credential Hardening); enforce CIS 5.2 (Use Unique Passwords) and CIS 6.5 (Require MFA for Administrative Access) across billing and geospatial system admin accounts; audit and remove any unauthorized accounts per NIST AC-2 (Account Management).
4. Recovery: Validate data integrity of billing records against known-good backups; confirm RTKBase configuration files have not been altered using D3-SFA (System File Analysis) and D3-SICA (System Init Config Analysis); restore access under NIST AC-3 (Access Enforcement) with least-privilege review per NIST AC-6 (Least Privilege) and D3-UAP (User Account Permissions); monitor outbound data transfer volumes for 30 days post-remediation.
5. Post-Incident: Conduct a gap assessment against NIST AC-4 (Information Flow Enforcement) to evaluate whether billing and OT/ICS network segments are adequately isolated; formalize an open-source software inventory for platforms like RTKBase per CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.2 (Ensure Authorized Software is Currently Supported); document lessons learned and update incident response playbook to address hacktivist exfiltration scenarios targeting public utility infrastructure.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if forensic analysis confirms any outbound transfer exceeding 1 GB to non-US IP space, if RTKBase configuration tampering is detected that could affect GNSS reference station integrity, or if PII or payment card data exfiltration is substantiated — triggering California Civil Code §1798.82 breach notification obligations and potential CPUC reporting for a Class A water utility.

Recovery Notes	Before restoring billing system access, validate database record integrity against the most recent pre-incident backup and confirm no unauthorized schema changes, triggers, or stored procedures were introduced by Handala that could enable persistent data access or exfiltration. RTKBase GNSS configuration files and mountpoint definitions must be hash-verified against known-clean baselines before the platform is returned to service, as tampered GNSS reference data could have downstream accuracy implications for any dependent surveying or infrastructure workflows. Maintain enhanced outbound transfer monitoring and anomalous authentication alerting for a minimum of 30 days post-remediation, as Handala has historically maintained persistent access in claimed operations before public disclosure.
Forensic Artifacts	RTKBase web server access logs (/var/log/nginx/access.log or /var/log/apache2/access.log): look for high-frequency requests from non-US IPs to the RTKBase web UI or NTRIP caster endpoint, abnormally large response sizes indicating bulk GNSS data pulls, and POST requests to admin/configuration endpoints outside business hours | Billing system database transaction logs (MySQL General Query Log or MSSQL Trace/Audit Log): search for SELECT * or SELECT INTO OUTFILE queries against customer, payment, or account tables, particularly queries returning >10,000 rows or generating flat-file exports — consistent with the claimed 5 GB bulk exfiltration of customer billing records | Windows Security Event Log (Event IDs 4624 Type 3/10, 4648, 4720, 4732) and Linux /var/log/auth.log on billing and RTKBase hosts: identify logon events from Iranian ASN IP blocks (AS44244 Shatel, AS197207 Mobile Communication Company of Iran, AS16322 Pars Online) or anonymization infrastructure (Tor exit nodes, commercial VPS ranges) correlated to the Handala operational window | RTKBase configuration files and SSH authorized_keys (/etc/rtk/*.conf, /home/[user]/.ssh/authorized_keys, /etc/sudoers): hash-compare against vendor baseline to detect Handala-implanted backdoor SSH keys, modified admin credentials, or added cron jobs used for persistence or scheduled exfiltration | Outbound NetFlow or proxy logs (or Windows Firewall log at %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log): filter for sustained outbound TCP sessions >500 MB to non-CDN, non-vendor destinations, particularly to cloud storage or paste-service endpoints consistent with Handala's documented use of Telegram and public file-sharing platforms for exfil staging and data publication

Per-Action IR Details

Containment — Audit and restrict external access to billing system interfaces and any internet-exposed RTKBase GNSS instances; enforce NIST AC-17 (Remote Access) by reviewing and tightening remote access policies; apply CIS 4.4 and CIS 4.5 to verify firewall rules block unauthenticated access to billing and geospatial platforms.

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run 'netstat -ano' or 'ss -tulnp' on billing system and RTKBase hosts to enumerate all listening services and active external connections. Use UFW or iptables to immediately block all non-essential inbound ports to RTKBase (default port 2101 NTRIP, 8080/8443 web UI) and billing system interfaces. On Windows billing hosts, run 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' and cross-reference remote IPs against known Iranian ASN blocks (e.g., AS44244, AS197207) using a free IP-to-ASN lookup.

Evidence: BEFORE restricting access or modifying firewall rules, capture: (1) full memory dump of billing system and RTKBase application servers using WinPmem or LiME to preserve in-memory session tokens, active database connections, and any staged exfil processes; (2) 'netstat -ano' / 'ss -tulnp' output showing all established connections, particularly any persistent outbound connections to non-US IP ranges; (3) RTKBase web server access logs (typically

/var/log/nginx/access.log or /var/log/apache2/access.log) showing recent client IP history and URI patterns; (4) current firewall rule sets ('iptables -L -n -v' or Windows Firewall export) as a before-state baseline.

Detection — Review authentication logs on billing system and RTKBase hosts for anomalous logins, large data transfers, or access from Iranian IP ranges; apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) to search for T1078 (Valid Accounts) and T1567 (Exfiltration Over Web Service) indicators; enable D3-LAM (Local Account Monitoring) to surface unauthorized local account activity; query for bulk SELECT queries or export events against billing database tables in the relevant timeframe.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records)

Compensating: On Windows billing hosts, query Security Event Log for Event ID 4624 (successful logon) and 4625 (failed logon) filtered to Type 3 (network) and Type 10 (remote interactive) — correlate source IPs against Iranian ASN ranges. For RTKBase (Linux), parse /var/log/auth.log for SSH successes and failures. For the billing database, enable and query the MySQL General Query Log or MSSQL Audit Log for SELECT *, OUTFILE, or BACKUP DATABASE commands. Use 'journalctl -u rtkbase --since "2025-01-01"' to recover RTKBase service activity. Deploy Sysmon with SwiftOnSecurity config to capture Event ID 3 (network connections) and Event ID 11 (file creation) going forward.

Evidence: This step is analytical and does not alter live state, but evidence collection should include: (1) Windows Security Event Log exports (Event IDs 4624, 4625, 4648, 4720, 4732) from billing system hosts covering the 90-day window preceding Handala's claim; (2) RTKBase application logs and NTRIP caster logs showing connected client IPs and data streamed — exfil of GNSS data would appear as abnormally high-volume RTCM3 stream pulls from unrecognized mountpoints; (3) billing database transaction logs or slow query logs showing unusually large result sets or export-to-file operations against customer PII tables (e.g., account, payment, customer tables); (4) outbound NetFlow or proxy logs showing transfers >100 MB to non-CDN, non-vendor external IPs, consistent with the claimed 5 GB exfil.

Eradication — Rotate all credentials associated with billing system service accounts and RTKBase platform per D3-CRO (Credential Rotation) and D3-CH (Credential Hardening); enforce CIS 5.2 (Use Unique Passwords) and CIS 6.5 (Require MFA for Administrative Access) across billing and geospatial system admin accounts; audit and remove any unauthorized accounts per NIST AC-2 (Account Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Export all local and domain accounts on billing hosts via 'Get-LocalUser' and 'Get-ADUser -Filter *' (or 'getent passwd' on Linux RTKBase hosts) and manually audit against the authorized account list. Identify and immediately disable any accounts created after the earliest plausible compromise date. For RTKBase, inspect /etc/passwd and /etc/sudoers for unauthorized entries. Rotate service account passwords using a password manager (Bitwarden free tier acceptable); document each rotation with timestamp. For MFA on RTKBase web UI, configure Google Authenticator via PAM ('libpam-google-authenticator') if native MFA is unsupported.

Evidence: BEFORE rotating credentials, capture: (1) full export of /etc/passwd, /etc/shadow, /etc/sudoers, and ~/.ssh/authorized_keys on all RTKBase and billing Linux hosts — Handala may have implanted an SSH backdoor key; (2) Windows Security Event Log Event ID 4720 (account created), 4722 (account enabled), 4728/4732 (member added to privileged group) to identify any accounts Handala may have created or elevated during the intrusion; (3) 'net user /domain' and 'Get-ADGroupMember -Identity Administrators' output as a point-in-time snapshot before any account removals; (4) RTKBase configuration file /etc/rtk/users.conf or equivalent storing platform-level credentials, preserved as forensic evidence before modification.

Recovery — Validate data integrity of billing records against known-good backups; confirm RTKBase configuration files have not been altered using D3-SFA (System File Analysis) and D3-SICA (System Init

Config Analysis); restore access under NIST AC-3 (Access Enforcement) with least-privilege review per NIST AC-6 (Least Privilege) and D3-UAP (User Account Permissions); monitor outbound data transfer volumes for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-11 (Audit Record Retention), CIS 3.4 (Enforce Data Retention)

Compensating: Use 'sha256sum' or 'Get-FileHash' to hash-compare RTKBase binaries and configuration files (rtknavi.conf, str2str configs, mountpoint definitions) against vendor-distributed checksums or a known-clean backup taken before the claimed breach window. For billing database integrity, run row-count and checksum queries against critical tables (customer, payment, account_balance) and compare against the most recent verified backup. Deploy a lightweight outbound bandwidth monitor (vnstat on Linux, or Windows Performance Monitor with a 'Network Interface Bytes Sent/sec' alert threshold) to flag post-remediation exfil attempts consistent with a persistent implant that survived initial eradication.

Evidence: This step restores live system state — before restoring from backup or modifying access controls, capture: (1) forensic images (dd or FTK Imager) of compromised billing system disk volumes and RTKBase host storage as legal-hold evidence, since Cal Water is a publicly traded utility and breach disclosure obligations may require preserved forensic evidence; (2) hash-verified copies of all RTKBase configuration files and binary executables in current (potentially tampered) state before overwrite; (3) current billing database snapshot in its potentially-modified state, preserving evidence of any Handala-inserted records, deleted rows, or schema changes that may be needed for regulatory disclosure or litigation.

Post-Incident — Conduct a gap assessment against NIST AC-4 (Information Flow Enforcement) to evaluate whether billing and OT/ICS network segments are adequately isolated; formalize an open-source software inventory for platforms like RTKBase per CIS 2.1 (Establish and Maintain a Software Inventory) and CIS 2.2 (Ensure Authorized Software is Currently Supported); document lessons learned and update incident response playbook to address hacktivist exfiltration scenarios targeting public utility infrastructure.

NIST Phase: Post Incident

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: Conduct a manual network segment review by mapping firewall rules between the billing VLAN, RTKBase GNSS network segment, and any OT/ICS (SCADA) network using Nmap ('nmap -sn' for host discovery, 'nmap -sV -p-' for service enumeration on the billing subnet boundary). Use the open-source RTKBase GitHub release history (github.com/Stefal/rtkbase) to verify the deployed version against the latest release and identify any known vulnerabilities. Document findings in a structured lessons-learned report referencing the Handala TTPs and submit to CISA's water sector ISAC (WaterISAC) for threat sharing under 6 USC §671 protections.

Evidence: Post-incident documentation artifacts to preserve and formalize: (1) complete timeline reconstruction correlating billing system authentication events, RTKBase access logs, and outbound transfer logs across the full intrusion window; (2) network topology diagram showing actual (vs. intended) connectivity between billing systems, RTKBase platform, and any OT/SCADA network segments — gaps discovered here are regulatory findings; (3) regulatory notification assessment documenting California data breach notification obligations under California Civil Code §1798.29 and §1798.82 (PII breach affecting CA residents), plus any CPUC reporting requirements applicable to a Class A water utility; (4) copy of updated IR playbook section covering hacktivist-attributed exfiltration targeting public utility billing and geospatial infrastructure.

Detection Guidance

Query authentication logs on billing system and RTKBase hosts for logins outside business hours, logins from unfamiliar geographic regions (particularly Iranian IP ranges), and service account logins not tied to scheduled processes (T1078). Search web server and application logs for large POST or GET requests consistent with bulk data staging or exfiltration (T1567, T1530). Apply NIST AU-6 to review audit records for high-volume database read operations or export events against customer PII tables. For RTKBase specifically, review configuration file modification timestamps and compare against D3-SFA (System File Analysis) baselines; check for new or altered startup configuration entries per D3-SICA. Monitor outbound traffic for sustained large transfers to unfamiliar external endpoints, consistent with T1567 (Exfiltration Over Web Service). CIS 8.2 (Collect Audit Logs) should be verified as active across all billing and geospatial platform hosts before triage begins. No confirmed IOCs (hashes, IPs, domains) have been publicly attributed to this specific incident; behavioral indicators above are derived from the mapped MITRE techniques.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.dataminr.com/resources/intel-brief/cyber-intel-brief-handala-claims-breach-of-california-water-service/`	Dataminr Intel Brief reporting Handala's claim — Tier 3 source, not an authoritative advisory	LOW
URL	`https://www.reddit.com/r/pwnhub/comments/1u3w10e/iranian_cyber_group_handala_claims_hack_of/`	Community aggregation of Handala claim — Tier 3 source, unverified	LOW

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1213** — Data from Information Repositories
- **T1566** — Phishing
- **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
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-3** — Access Enforcement
- **SC-28** — Protection of Information at Rest

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1213	Data from Information Repositories	Collection
T1566	Phishing	Initial-Access

Technique ID	Technique Name	Tactic
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
Cyber Intel Brief: Handala Claims Breach of California Water Service	https://www.dataminr.com/resources/intel-brief/cyber-intel-brief-ha...	T3
Leadership Team - California Water Service Group	https://www.calwatergroup.com/our-company/leadership-team	T3
California Water Service	https://www.calwater.com/	T3
Iranian Cyber Group Handala Claims Hack of California Water Service	https://www.reddit.com/r/pwnhub/comments/1u3w10e/iranian_cyber_grou.. .	T3
About - The Cal Water Difference	https://calwaterdifference.com/about/	T3

Generated 2026-06-14 13:36 UTC by TJS Security Command Center