INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 07:18 UTC

Data Breach at Crime Stoppers of Hamilton via Navigate360 Software

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0180
Type	Data Breach
Severity	HIGH
Affected Products	Navigate360 platform (version unspecified); Crime Stoppers of Hamilton deployment
Published	12 hours ago
Discovery Source	Serper

Executive Summary

Crime Stoppers of Hamilton disclosed a cybersecurity breach originating from their software vendor, Navigate360. The incident potentially exposes sensitive data held by a law enforcement-adjacent organization, including tipster submissions, which carry heightened confidentiality obligations and personal safety implications. Root cause, attack vector, and confirmed data types remain unverified pending Navigate360's formal incident report; risk scope is currently unknown.

Technical Analysis

Navigate360, a software platform used by Crime Stoppers of Hamilton, experienced a cybersecurity breach of undetermined technical origin. No CVE has been assigned, no CWE has been identified, and no MITRE ATT&CK techniques have been attributed as of available reporting. The affected version of Navigate360 is unspecified. Attack vector, exploitation method, and confirmed data categories have not been publicly disclosed. Crime Stoppers of Hamilton has formally requested a detailed incident report from Navigate360. Hamilton Police Service has been notified. The breach is being treated as a third-party software supply chain or hosted-platform incident; no independent technical indicators of compromise are publicly available. Patch status and vendor remediation guidance have not been published.

Action Checklist

1. Step 1: Containment. If your organization uses Navigate360, contact Navigate360 directly to determine whether your tenant or deployment was affected. Request written confirmation of scope and any emergency mitigation steps from the vendor. Suspend non-essential integrations with the Navigate360 platform until scope is confirmed.

2. Step 2: Detection. Review access logs for the Navigate360 platform for anomalous authentication events, data exports, or API calls outside normal business hours. Per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs), ensure logging is enabled and retained for the Navigate360 environment and any identity providers federated to it. Without published IOCs, behavioral anomalies are the primary detection signal.

3. Step 3: Eradication. Await Navigate360's formal incident report before scoping eradication. Per NIST IR-4 (Incident Handling), coordinate with the vendor to confirm whether the vulnerability or access path has been closed. If Navigate360 issues a patch or configuration change, apply it under NIST SI-2 (Flaw Remediation) procedures. Rotate credentials for all accounts with access to the Navigate360 platform per NIST SP 800-63B (credential rotation).

4. Step 4: Recovery. Validate that Navigate360 has confirmed remediation in writing before restoring full platform operations. Per NIST IR-5 (Incident Monitoring), continue monitoring for anomalous activity for a minimum of 30 days post-remediation. Verify that audit logging per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation) is capturing all post-recovery activity for forensic continuity.

5. Step 5: Post-Incident. Conduct a third-party vendor risk review against your existing vendor management framework. Per NIST IR-8 (Incident Response Plan), update your incident response plan to include vendor-originated breach scenarios. Evaluate whether contractual requirements for breach notification timelines and incident reporting are in place with Navigate360 and any comparable software vendors handling sensitive data.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if Navigate360 confirms that tipster submission records — including identity, contact information, or tip content — were accessible to unauthorized parties, triggering breach notification obligations under applicable state privacy law and heightened personal safety risk to tipsters who reported criminal activity.
Recovery Notes	Do not restore full Navigate360 platform access until Navigate360 provides written confirmation identifying the specific access path or vulnerability that was exploited and verifying it has been closed in your tenant. Post-restoration, monitor Navigate360 IdP sign-in logs and application audit logs daily for a minimum of 30 days, baselining against pre-breach access patterns and flagging any accounts, source IPs, or API call volumes that deviate from that baseline. Given the law enforcement-adjacent nature of this deployment and the sensitivity of tipster identity data, retain all incident-related logs for a minimum consistent with your jurisdiction's evidence retention requirements and coordinate record disposition with legal counsel before destruction.

Forensic Artifacts	Navigate360 platform application audit logs: specifically bulk record query events, data export operations, and API calls to tipster submission endpoints during the breach window — these would reflect the attacker's data access pattern within the SaaS platform. | Identity provider sign-in logs (Azure AD, Okta, or SAML IdP) for all accounts federated to Navigate360: filtering for the breach timeframe to identify which accounts authenticated, from what source IPs, and whether service accounts were used interactively — the primary indicator of credential compromise or session hijacking in a SaaS-origin breach. | OAuth token grant and API key issuance records for the Navigate360 tenant: unauthorized or anomalous token grants during the breach window would indicate the attacker established persistent API access to extract tipster data without repeated authentication. | Network egress and DNS logs from your environment showing connections to Navigate360 infrastructure: large outbound data volumes or connections from unexpected internal hosts to Navigate360 domains during the breach window would indicate lateral movement or unauthorized clients accessing the platform through your network. | Navigate360 vendor-provided breach scope confirmation and internal incident timeline documentation: the formal record of what data types were accessible, which tenants were affected, and the attack vector as disclosed by Navigate360 — essential for regulatory notification decisions and the post-incident legal record given the tipster safety implications.

Per-Action IR Details

Step 1: Containment — If your organization uses Navigate360, contact Navigate360 directly to determine whether your tenant or deployment was affected. Request written confirmation of scope and any emergency mitigation steps from the vendor. Suspend non-essential integrations with the Navigate360 platform until scope is confirmed.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Document all Navigate360 integration endpoints using your firewall or proxy configuration files (e.g., `grep -r 'navigate360' /etc/nginx/` or Windows hosts file review). Disable or firewall-block Navigate360 API endpoints and OAuth callback URIs at the perimeter using `iptables` or Windows Firewall rules while awaiting vendor confirmation. A 2-person team can enumerate active integrations by querying the identity provider (e.g., Azure AD: `Get-MsolServicePrincipal | Where-Object {$_.DisplayName -like '*Navigate360*'}`).

Evidence: Before suspending integrations or revoking API tokens, capture: (1) active authenticated sessions to the Navigate360 platform from your identity provider's sign-in logs (e.g., Azure AD Sign-In Logs filtered for Navigate360 application ID, Okta System Log filtered for `target.displayName eq 'Navigate360'`); (2) current OAuth token grants and API key inventory for the Navigate360 tenant; (3) network flow logs or firewall session tables showing active connections to Navigate360 infrastructure IPs/domains at the time of suspension. This preserves the pre-containment access baseline required to identify which accounts or systems were communicating with the compromised vendor environment.

Step 2: Detection — Review access logs for the Navigate360 platform for anomalous authentication events, data exports, or API calls outside normal business hours. Per NIST SI-4 (System Monitoring) and CIS 8.2 (Collect Audit Logs), ensure logging is enabled and retained for the Navigate360 environment and any identity providers federated to it. Without published IOCs, behavioral anomalies are the primary detection signal.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell to pull Azure AD or Okta logs for Navigate360 app sign-in events: `Get-AzureADAuditSignInLogs -Filter "appDisplayName eq 'Navigate360'" | Where-Object {$_.RiskLevelDuringSignIn -ne 'none'}`. For on-premise deployments, parse IIS or Apache access logs with `grep` or `awk` filtering for Navigate360 API paths, unusual HTTP methods (PUT, DELETE on tipster record endpoints), or large response body sizes indicating bulk data export. Use Microsoft Excel or `csvkit` to baseline authentication timestamps and flag after-hours or geographically anomalous sessions manually.

Evidence: Capture before any remediation action: (1) Navigate360 platform application-level audit logs covering the maximum available retention window — specifically bulk data export events, record query volumes above baseline, and API calls to tipster submission endpoints; (2) identity provider sign-in logs for all accounts federated to Navigate360 (Azure AD, Okta, or SAML IdP logs), filtered for impossible travel, unfamiliar device fingerprints, or service account logins from interactive sessions; (3) DNS query logs from your resolver showing Navigate360 domain lookups, which may reveal unauthorized clients querying the platform; (4) any WAF or reverse-proxy logs if Navigate360 is accessed through one, capturing request URI patterns and response sizes that would indicate mass record retrieval. Since no IOCs have been published, preserve the full log corpus before any retention policy purges it.

Step 3: Eradication — Await Navigate360's formal incident report before scoping eradication. Per NIST IR-4 (Incident Handling), coordinate with the vendor to confirm whether the vulnerability or access path has been closed. If Navigate360 issues a patch or configuration change, apply it under NIST SI-2 (Flaw Remediation) procedures. Rotate credentials for all accounts with access to the Navigate360 platform per D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Credential rotation for a 2-person team without PAM tooling: export the full account list with Navigate360 access from your IdP (`Get-MsolUser | Where-Object {$_.Licenses -ne $null}` or Okta Users API filtered by Navigate360 app assignment), then reset passwords and revoke all active sessions via IdP admin console. For service accounts or API keys embedded in integrations, locate them by searching config files and environment variables (`grep -rn 'navigate360\|n360' /etc/app-config/` or Windows Registry search using `reg query HKLM /f navigate360 /s`). Disable and reissue rather than rotate in-place to ensure the original compromised credential is fully invalidated.

Evidence: Before rotating any credentials or applying vendor patches, capture: (1) a full export of currently active sessions and OAuth grants for all accounts with Navigate360 access — this is volatile and destroyed upon rotation; (2) the pre-patch Navigate360 application version string and configuration state (screenshot or exported config) to document the vulnerable state for the incident record; (3) any Navigate360 application-level audit entries showing the last successful authentication for each account, establishing the forensic baseline before credentials are invalidated. Credential rotation and patch application alter live authentication state — this evidence must be preserved first per RFC 3227 / NIST 800-61r3 order of volatility.

Step 4: Recovery — Validate that Navigate360 has confirmed remediation in writing before restoring full platform operations. Per NIST IR-5 (Incident Monitoring), continue monitoring for anomalous activity for a minimum of 30 days post-remediation. Verify that audit logging per AU-2 (Event Logging) and AU-12 (Audit Record Generation) is capturing all post-recovery activity for forensic continuity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-11 (Audit Record Retention), CIS 8.2 (Collect Audit Logs)

Compensating: Without enterprise SIEM, establish a manual 30-day monitoring cadence: schedule a daily cron job or Windows Task Scheduler script to pull Navigate360 IdP sign-in logs and email a summary of new accounts, after-hours logins, and bulk export events to the IR team. Use `diff` or PowerShell `Compare-Object` against the pre-breach account and permission baseline you captured during detection to flag any unauthorized changes that persist

post-remediation. Retain all logs locally to an append-only directory (`chattr +a /var/log/navigate360/` on Linux) to satisfy forensic continuity requirements for law enforcement-adjacent data.

Evidence: At recovery initiation, document: (1) Navigate360's written remediation confirmation including the specific vulnerability or access path closed, patch version applied, and the vendor's confirmed scope of affected tenants — this is the formal record establishing the eradication boundary; (2) a post-remediation snapshot of the Navigate360 audit log configuration showing that logging is active and shipping to a retained location, confirming forensic continuity is not broken by the platform restoration; (3) a re-baseline of normal authentication patterns (login times, source IPs, API call volumes) against which the 30-day monitoring window will be measured. Because this incident involves potential exposure of tipster identity data, the evidence record must support any future law enforcement or regulatory review.

Step 5: Post-Incident — Conduct a third-party vendor risk review against your existing vendor management framework. Per NIST IR-8 (Incident Response Plan), update your incident response plan to include vendor-originated breach scenarios. Evaluate whether contractual requirements for breach notification timelines and incident reporting are in place with Navigate360 and any comparable software vendors handling sensitive data.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: A 2-person team can conduct vendor risk review using the free CIS Controls v8 Self-Assessment Tool (CIS CSAT) to score Navigate360 against IG1 safeguards, or apply the CISA Tabletop Exercise Package (CTEP) template adapted for third-party breach scenarios — both are publicly available at no cost. Document findings in a vendor risk register (a versioned spreadsheet suffices) tracking: Navigate360 breach notification timeline from event to customer disclosure, contractual SLA for incident reporting, data types processed, and remediation evidence received. For law enforcement-adjacent organizations handling tipster data, flag this review for legal counsel given the heightened confidentiality and potential witness safety obligations.

Evidence: Compile the post-incident record package: (1) the full Navigate360 vendor communication timeline from initial breach notification to written remediation confirmation, timestamped; (2) the incident log documenting all detection, containment, and eradication actions taken by your organization with timestamps and responsible parties, satisfying NIST IR-5 (Incident Monitoring) documentation requirements; (3) a lessons-learned report specifically addressing the gap between Navigate360's breach occurrence and your organization's notification — this gap is the primary control failure to remediate in the updated IR plan under NIST IR-8 (Incident Response Plan). Because tipster identity data carries law enforcement sensitivity, retain the complete incident record per your jurisdiction's evidence retention requirements and coordinate with your legal team on mandatory breach notification obligations before closing the incident.

Detection Guidance

No IOCs, MITRE techniques, or vendor-published indicators are available as of current reporting. Detection relies on behavioral and access-pattern analysis. Review Navigate360 platform authentication logs for credential stuffing patterns, unexpected administrative logins, or bulk data access events. Cross-reference against identity provider logs (SSO, LDAP, or SAML federation logs) for anomalous session creation. Per NIST AU-6 (Audit Record Review, Analysis, and Reporting), review audit records for the Navigate360 deployment at increased frequency until vendor scope confirmation is received. If Navigate360 is hosted as SaaS, request platform-side access logs directly from the vendor. Per CIS 8.2 (Collect Audit Logs), confirm logging is enabled at the enterprise asset level for any systems integrated with Navigate360. Monitor local account activity per NIST AU-2 (Event Logging) for any on-premise components. No specific log queries, event IDs, or hash-based IOCs can be provided from available source material.

Framework Mappings

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **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

Sources

Source	URL	Tier
	https://www.flamboroughtoday.com/police-beat/cybersecurity-breach-r...	T3
Hamilton Police Made Aware of Crime Stoppers Breach	https://hamiltonpolice.on.ca/news/hamilton-police-made-aware-of-cri...	T3
Hamilton Police Made Aware of Crime Stoppers Breach - Facebook	https://www.facebook.com/DanWiestAroundTheCommunity/photos/hamilton...	T3
Will we ever hear details about the City's Cybersecurity incident?	https://www.reddit.com/r/Hamilton/comments/1kt0nqe/will_we_ever_hea...	T3
Cyber Crime - Crime Stoppers Hamilton	https://crimestoppershamilton.com/cyber-crime/	T3

Generated 2026-06-18 07:18 UTC by TJS Security Command Center