GhostTrace LLC

Security Incident Report

Report published	July 9, 2026
Incident date	July 9, 2026
Classification	Public
Prepared by	GhostTrace LLC

Executive Summary

On July 9, 2026, GhostTrace LLC identified and responded to a coordinated attempt to abuse several features of its public-facing platform. This included an attempt to use a webhook/integration feature to direct our own server to make requests to internal or restricted network destinations (a technique known as Server-Side Request Forgery, or SSRF), an attempted cross-site-scripting (XSS) injection, automated creation of platform accounts, and abusive and defamatory content posted to an internal notification channel through a compromised third-party credential. GhostTrace identified this activity through its own internal activity logging, contained it the same day, and has since deployed a substantial set of new security controls, described below. **GhostTrace found no evidence that any customer data, case files, or payment information were accessed by the responsible party or parties.**

What Happened

GhostTrace's public platform includes several features available to registered accounts, including a webhook/integration tool that lets an account receive automated notifications at a URL of their choosing, a document-upload feature for account records, and a public form for anonymous tips. GhostTrace's investigation found that an actor, operating from network infrastructure associated with the Tor anonymity network, registered a platform account and used it to:

- Register two outbound webhook destinations pointed at third-party request-logging services — activity consistent with reconnaissance of the webhook feature, and which led to the discovery described below.
- Attempt to upload an account document containing a cross-site-scripting (XSS) payload in its title.
- Submit false, abusive content through GhostTrace's public tip-reporting form.

Separately, and on the same day, a webhook credential connected to an internal Discord notification channel was used by an unknown party to post abusive, defamatory, and graphic content targeting a GhostTrace executive. GhostTrace's investigation found no indication that this credential was exposed through any GhostTrace application code, source repository, or API response — Discord webhook URLs of this kind are never transmitted to or displayed in any customer- or public-facing part of the platform. The exposure is understood to have originated outside GhostTrace's own systems.

Also on the same day, GhostTrace identified a wave of automated account-creation attempts made directly against the authentication provider used by the platform, separate from the path most users use to register.

On attribution. Several signals — network origin, timing, and technique — suggest some or all of this activity may be connected. GhostTrace has not established definitive proof linking every event described here to a single individual, and this report does not claim to.

Timeline

Time (ET)	Event
Earlier that day	A submission was made through GhostTrace's public tip-reporting form containing false, abusive content unrelated to any genuine report.
1:53 PM	A platform account was registered from network infrastructure associated with the Tor anonymity network.
2:00 – 2:01 PM	The same account registered two outbound webhook destinations pointed at third-party request-logging services.
2:11 PM	The same account attempted to upload a document containing an XSS payload in its title field.
Later that day	A webhook credential connected to an internal Discord channel was used to post abusive, defamatory, and graphic content. GhostTrace staff deleted the channel and revoked/rotated affected webhook credentials immediately upon discovery.
Later that day	GhostTrace staff, reviewing platform activity logs, identified the pattern of activity described in this report, took the public website offline as a precaution, and began remediation.
Later that day	A wave of automated account-creation attempts was identified against the platform's authentication provider.
Same day	All identified vulnerabilities were corrected and the additional protections listed below were deployed. The website was brought back online.

On precision. Times shown are drawn directly from GhostTrace's activity logs where available. Events without a logged timestamp are described in relative order rather than with an invented time.

Our Investigation and Response

- Deleted the affected Discord channel and revoked/rotated the Discord webhook credentials in use, immediately upon discovery.
- Reviewed whether the exposed credential originated from GhostTrace's own systems; confirmed it does not appear anywhere in the platform's source history or in any API response reachable by a user.
- Reviewed the platform's activity logs, which record the network origin of account and integration activity, to reconstruct the timeline above.
- Identified and corrected the Server-Side Request Forgery (SSRF) weakness in the webhook/integration feature: outbound destinations are now validated, and requests to private, internal, or reserved network addresses are refused before they are ever made. This closes a technique attackers commonly use to reach cloud infrastructure metadata and internal services.
- Confirmed, through direct code review, that the attempted XSS injection could not have executed: the affected field is rendered as plain text everywhere it is displayed on the platform.

- Found no evidence, in the platform's logs or in the affected systems, that any customer data, case files, payment information, or internal systems were accessed.

Security Enhancements Implemented

- Closed the SSRF vulnerability described above, with validation enforced both when an integration is created and again each time it is used, to prevent bypass via delayed network changes.
- Added rate limiting and bot-verification (Google reCAPTCHA-based) to account-creation flows, including the path used to create accounts through our authentication provider directly — closing the gap that allowed automated account creation.
- Deployed IP-address and device-level blocking, enforced platform-wide before any request reaches application logic, with a staff-managed review interface.
- Deployed automatic detection of traffic originating from the Tor anonymity network, VPNs, and open proxies, now enforced on account creation, document uploads, integration/webhook creation, and tip submissions.
- Deployed automatic detection and blocking of known network-scanning tools.
- Deployed an automated review queue that surfaces suspicious activity — including blocked intrusion attempts and content matching common attack patterns — together with the originating IP address and a persistent device signal, so staff can dismiss, block, or disable related accounts immediately.
- Added a persistent device-identification signal, independent of IP address, to reduce the effectiveness of simply switching networks to evade a block. This is not a hardware identifier — no website can access one, by design of every modern browser — but it meaningfully raises the bar for repeat abuse from the same device.
- Required a verified email address before any newly created account can take any action beyond viewing its own information.
- Expanded internal activity logging to include the device signal above and automatic flagging of known anonymization-network traffic, to support faster investigation of any future incident.
- Conducted an expanded internal review of account permissions and data-access controls across the platform, and corrected two additional issues identified during that review before they were ever reported as exploited.
- Added encryption at rest for the most sensitive stored files (account documents and submitted evidence) and enabled HTTP Strict Transport Security (HSTS) to prevent downgrade to an unencrypted connection.

Impact Assessment

- No evidence of unauthorized access to customer data, case files, payment records, or credentials.
- The abusive content posted to the internal Discord channel was not visible to customers or the public; the channel and its content were removed immediately upon discovery.

- As a precaution, GhostTrace temporarily took its public website offline while the investigation and remediation were completed. GhostTrace runs paid search advertising and organic search traffic to the site; during the offline window, previously scheduled advertising continued to direct visitors to a site that was unavailable, resulting in wasted advertising spend and lost inquiries. GhostTrace is finalizing the exact financial impact internally and has not included an estimate in this public report in order to avoid publishing an unconfirmed figure.
- To GhostTrace's knowledge, no customer was contacted with fraudulent communications as a result of this incident.

A Note on Redactions

This report omits the specific network addresses, account identifiers, and the literal abusive content involved. This is deliberate: publishing that information would serve no protective purpose for our customers or the public, and could itself facilitate misuse. GhostTrace retains full unredacted records internally.

Our Commitment Going Forward

GhostTrace exists to help people who have been targeted by scams, harassment, and online abuse — we hold ourselves to the same standard of transparency and accountability we ask of the platforms and institutions we investigate on our clients' behalf. We are continuing to invest in the security of our platform and will disclose any future incident that meets this bar for public reporting.

Reporting Security Issues

If you have information about a security issue affecting GhostTrace, please contact **tech@ghosttrace.net**. We welcome responsible disclosure and will respond promptly.
