ObservePoint

# Security Incident Report

**Incident type**: Unauthorized Database Access + Data Breach

**Incident Date**: February 24, 2026

**Status**: Resolved

## Summary

This report describes unauthorized access to an ObservePoint database that took place on February 24, 2026, which resulted in a data breach. The purpose of this report is to inform customers about what happened as quickly as possible with full transparency. We consider the incident resolved.

### What Is ObservePoint?

Businesses use ObservePoint to audit their websites as a synthetic visitor and report information about their web pages (not their website visitors) including technologies loading on each page, cookies, accessibility issues, and page speed. ObservePoint does not collect personal information or information about the customers of our customers (such as website visitors).

### Why Now?

Our goal is to promptly inform ObservePoint customers of any security incident, so you can make decisions without undue delay. We are providing you with the current information we have, and we are confident the information in this report is accurate.

We have high confidence that the issue has been resolved. However, we are currently evaluating whether this incident justifies engaging a third-party security firm to perform forensic analysis of our systems. If we choose to engage a third-party firm and their findings yield additional details that would benefit customers, we will release an updated incident report.

### What We Know

On February 24, an unauthorized user gained access to an ObservePoint database through a stolen credential. On February 25, ObservePoint detected the unauthorized access, deactivated the stolen credential, and rotated all other credentials used to secure ObservePoint data. The affected database was a data warehouse used for business intelligence and reporting within the ObservePoint application. The next section describes the data that was accessed.

## Scope of Impact: What data was accessed

The scope of the unauthorized user's activities was limited to data access. The user did not interrupt any ObservePoint functionality, did not execute any code, and did not perform a

ransomware/encryption attack. None of the unauthorized user's actions were visible to ObservePoint customers.

The following lists describe all the data accessed by the unauthorized user. The list applies to past and present ObservePoint users, except past users who explicitly asked us to delete their account data.

We are sharing this information with as much detail as possible, so you can decide what actions are most appropriate for your organization.

**Your ObservePoint User Information**

*Note: these are your business users. ObservePoint does not store information about your customers or website visitors.*

- First Name
- Last Name
- Email Address
- ObservePoint Username
- Last Login Date
- Timezone
- Company Name

**Your ObservePoint Configurations**

- Sub-Folder Names (but not Folder names)
- Configuration information about Audits and Journeys:
    - Audit and Journey Names
    - Dates: Last Run Date, Last Edit Date, Next Run Date
    - Configured Browser Width & Height
    - Configured Webhook URL
    - Configured GPC Setting (on vs. off)
    - Configured Maximum Number of Pages
    - Configured Custom Proxy URL, if any
    - Email Addresses Subscribed to Audit, Journey, and Email Link Validation Notifications (even if they do not have an ObservePoint account)
    - Audit and Journey Notes (we recommend reviewing these notes for sensitive customer information)

**Credentials**

- Webhook Signing Secrets
    - These are keys used to apply digital signatures to webhooks delivered by ObservePoint to customers to ensure authenticity of the message. These credentials are **not** used to log in to ObservePoint or authenticate users.
    - Affected users should rotate their webhook signing secrets immediately. Instructions here.
    - **Action:** We have reached out to you individually if you are affected.
- User Password Hash
    - This does not apply to customers using Single Sign-On
    - The hashes are PBKDF2, and are salted
    - While there is low risk an attacker could recover a user's password from the hash, we took the proactive action of forcing all users to reset their password on next login, to mitigate the risk of an attacker gaining access to your ObservePoint account.

    - **Action:** No action required.
- Public Single Sign-On Certificates
    - Each ObservePoint account (organization) that uses SSO has a public certificate.
    - These certificates are generally considered public information, and are used to securely identify SAMLv2 identity providers when ObservePoint users log in via SSO.
    - These certificates are not *user* credentials and are not used to authenticate individual users.
    - **Action:** No action required, but if you would like to rotate your SSO certificate for ObservePoint, your IT team can do so via ObservePoint's self-service SSO feature. Instructions here.
- Masked Input Encryption Keys
    - These keys are managed by ObservePoint and not visible to customers. They are used to encrypt masked inputs at rest in web journeys and audit actions. The masked inputs themselves were not accessed by the attacker, but out of an abundance of caution, we have proactively rotated all of these keys and re-encrypted all masked inputs for customers.
    - No action is required. The attacker did not access your masked inputs, and we have proactively rotated these keys, such that the keys the attacker accessed are useless.
    - **Action:** No action required, but you have the option to rotate your masked inputs even though the unauthorized user did not access them.

**The unauthorized user did not access the following:**

- Audit and Journey Results, such as Page URLs, Cookies, Tags, etc.
- Audit and Journey Starting URLs
- Alert Configurations
- Consent Category Configurations
- Tag and Variable Rules
- Unapproved Cookie Lists
- Financial or health information such as credit card information (ObservePoint does not store any financial or health information)
- Anything else not mentioned in the previous section

# Timeline

This section describes the sequence of events that led to the unauthorized access, and the actions ObservePoint took to resolve the issue:

- **February 17, 2026** at **14:53 UTC**
  An unauthorized user logged in to the affected ObservePoint database using stolen credentials, but did not view any data. We presume this was a test to verify the stolen credentials. Our systems did not detect the unauthorized login at this time.

- **February 24, 2026** from **03:37** to **04:09** and **08:05** to **08:31 UTC**
  An unauthorized user exfiltrated the data described above, between two sessions that lasted 32 minutes and 26 minutes, respectively. The attacker attempted to escalate privileges, but failed because their credentials were limited to read-only access.

- **February 25, 2026** at **17:48 UTC**
  ObservePoint discovered the unauthorized access and deactivated the stolen credentials. ObservePoint rotated all credentials used to access ObservePoint systems, including the affected database and all other ObservePoint systems. From this point forward, ObservePoint continued investigating.

- **February 26, 2026** at **17:30 UTC**
  ObservePoint notified customers that unauthorized access had occurred while the investigation continued.

# Root Cause Analysis

Based on the evidence we have collected, we believe the attacker acquired an ObservePoint database credential through a general-purpose “infostealer” malware attack that exfiltrated the credential from an engineer’s workstation. The engineer was authorized to have this credential as part of their assigned duties working on infrastructure tasks. We believe the credential subsequently got into a data set of stolen credentials and later used by an automated system such as UNC5537 to steal information from many organizations. We believe this attack was not specifically designed to target ObservePoint. While the affected database requires multi-factor authentication for other credentials, this particular credential was not in use, planned to be deprecated, did not require MFA, and had not been rotated. Consequently, the attacker was able to log in to the database without a 2nd factor of authentication. We have corrected all of these gaps.

This style of stolen credential attack has affected hundreds of organizations, and we are taking measures to prevent it from affecting ObservePoint in the future by following security guidance from the database vendor (see the next section).

# Security Status: Is ObservePoint secure now?

We consider this issue resolved, and all known security gaps are closed.

We have taken the following steps to secure ObservePoint customer data from future attack:

- Rotated all credentials that have access to ObservePoint systems, including the affected database and all other ObservePoint systems. We specifically deactivated the credential that was used to gain this unauthorized access.
- We analyzed access logs to ensure no other unauthorized access has taken place.
- Applied security policies to add extra layers of defense, including network policies and MFA where it was missing.
- Audited all credential storage systems to ensure they are secure and have not experienced unauthorized access.
- Audited all engineering workstations for unauthorized credentials.
- Audited endpoint protection logs across all workstations.
- Implemented new procedures to fill gaps detected during this incident.

We are confident these steps will secure ObservePoint from this type of attack in the future, and many other types of attacks.

# Next Steps

The purpose of this document is to give you all the information they need to make informed decisions about how to respond to this incident. You may wish to share this document with your organization's security team.

We suggest you review the “Scope of Impact” section above, and determine what steps make sense for your organization. Note that ObservePoint has taken all the proactive steps possible to secure your data, but deciding what actions are necessary for your organization will vary.

If you have any questions, please contact support@observepoint.com.

# FAQ

### Did I cause this incident?

No. This incident was not caused by the actions of an ObservePoint user, or any organization with a relationship with ObservePoint.

### What do I need to do next?

Review this information to determine how you might be affected and what actions may be necessary. You may wish to share this information with your security team.

### Does ObservePoint perform regular security audits?

ObservePoint is SOC2 Type-2 certified and additionally performs regular penetration tests. In response to this incident, we are adding new steps to our regular security audits.

### What if I’m not currently an ObservePoint customer?

If you are not currently an ObservePoint customer or free account holder, and never have been, you are not affected. If you are a former customer, and you asked us to remove the data associated with your account, you are not affected. If you are a former customer, and you have not asked us to remove the data associated with your account, you may be affected. Please review this document carefully.

### What if I have a free ObservePoint account?

The unauthorized access included the same data listed above for free accounts.

### Was this a targeted attack against ObservePoint?

Based on the data access patterns we analyzed from the unauthorized user, we believe this attack was **not** targeted at ObservePoint specifically. Instead, it appears to be a general purpose automated mechanism that searches for contact information and credentials in database table and column names, similar to other common attacks that have unfortunately become prevalent on the internet in recent years. This conclusion is based on the order of tables accessed, table names, and other conspicuous facts that look like a mechanised process rather than a bespoke attack on ObservePoint’s specific data.

### What country and ISP did the attack originate from?

We consider the specific location and providers where the attack originated to be sensitive information. We have reported the activity to the hosting providers, and the providers have acknowledged the report.

### I use a VPN with ObservePoint. Is my VPN compromised?

No. No VPN information was accessed during the attack. VPN information is stored in a separate system that the attacker did not have access to.

### Should I block access to ObservePoint for users on my corporate network?

No. Since there is no active attack, blocking access for your users will give no security benefit.

### Was the attacker able to escalate privileges or do anything else inside the ObservePoint network?

No. The attacker only had access to a single database. Within the database, the attacker did not have permissions to escalate privileges, and logs clearly indicate that they did **not** escalate. Further, the attacker **did not access** any other networks where ObservePoint operates, including the networks where ObservePoint operates its scans, or any other ObservePoint infrastructure. The attacker did not have the ability to execute code or move laterally within the ObservePoint system. The attacker was not able to escalate privileges or change any data in ObservePoint's database.

### Did the attacker delete any data, encrypt any data, or perform a "ransomware" attack?

No. The forensics are clear that the attacker only viewed data, and did not modify any data or encrypt any data.

### Did the incident reduce ObservePoint's ability to monitor or troubleshoot?

No. All monitoring and troubleshooting tools remain intact and effective.

### Did this incident give an attacker access to any ObservePoint customer network, data, or systems?

No. This incident was limited in scope to a single ObservePoint database. From this database, there is no connectivity, directly or indirectly, to any customer network, customer data, customer systems, or any other customer information technology asset.