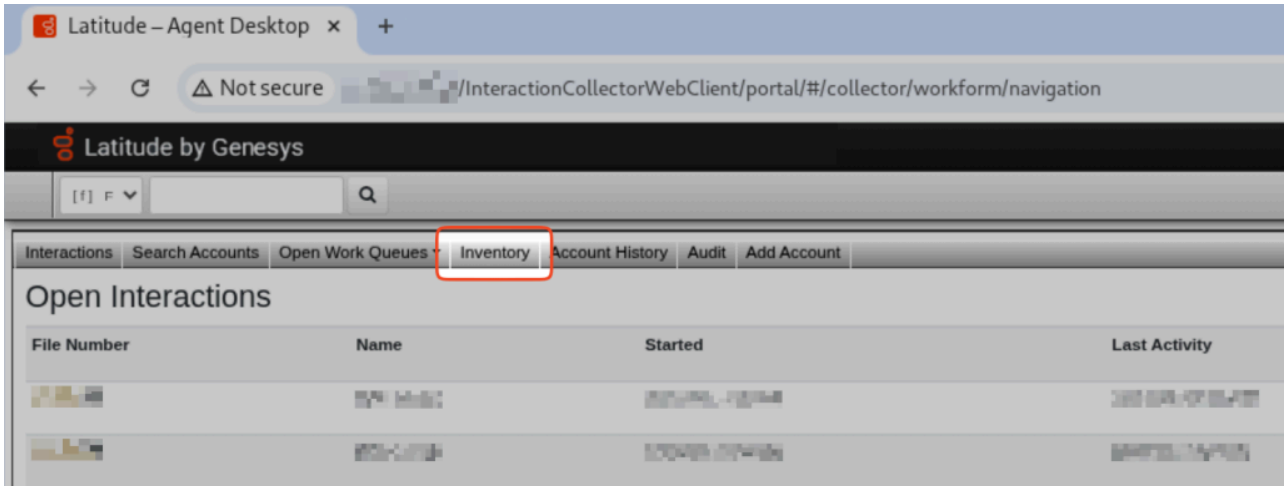
CVE-2025-70420: Authenticated SQL Injection in Genesys Latitude

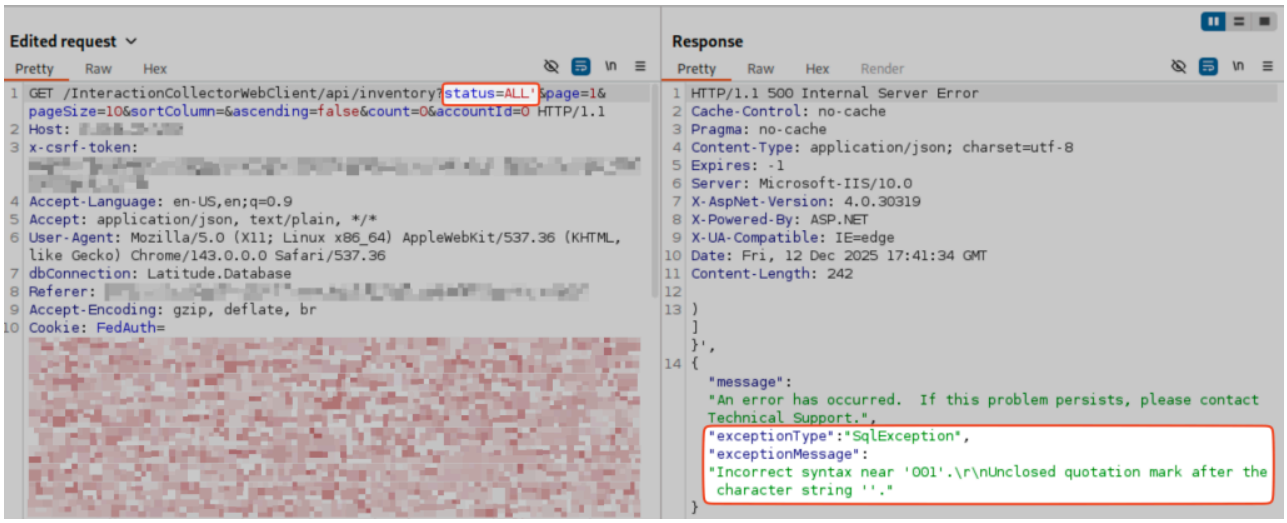
Disclosures

During a security assessment, OkunSec identified an authenticated SQL injection vulnerability in Latitude v25.1.0.420, developed by Genesys. Latitude is a debt collection platform used to manage accounts, process payments, and handle debtor communications. As such, it processes sensitive PII and financial data, making it an attractive target for threat actors.

The issue was identified in the status parameter of the /InteractionCollectorWebClient/api/inventory endpoint, which can be accessed via the “Agent Desktop” navigation menu and clicking the “Inventory” link.



We observed that appending a single quote to the parameter value triggered a database error, indicating improper input handling.



Using SQLMap, we automated the injection and were able to enumerate the database system, including its version and databases.

```
[13:35:07] [INFO] the back-end DBMS is Microsoft SQL Server
back-end DBMS: Microsoft SQL Server 2019
[13:35:07] [INFO] fetching database names
[13:35:07] [INFO] resumed: 'Latitude'
[13:35:07] [INFO] resumed: 'master'
[13:35:07] [INFO] resumed: 'model'
[13:35:07] [INFO] resumed: 'msdb'
[13:35:07] [INFO] resumed: 'tempdb'
[13:35:07] [INFO] resumed: 'Token2'
available databases [6]:
[*] Latitude
[*] master
[*] model
[*] msdb
[*] tempdb
[*] Token2

[13:35:07] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 1 times
[13:35:07] [INFO] fetched data logged to text files under '/home/kali/.local/
```

While the injection worked, we were unable to extract sensitive data from the “Latitude” table, likely due to extra protections at the database layer.

Disclosure Timeline

- 2025-12-10 — Vulnerability discovered and client notified
- 2025-12-23 — Vendor notified (first attempt)
- 2026-01-30 — Vendor notified (second attempt)
- 2026-03-18 — Vendor notified (third attempt)
- 2026-04-21 — Public disclosure