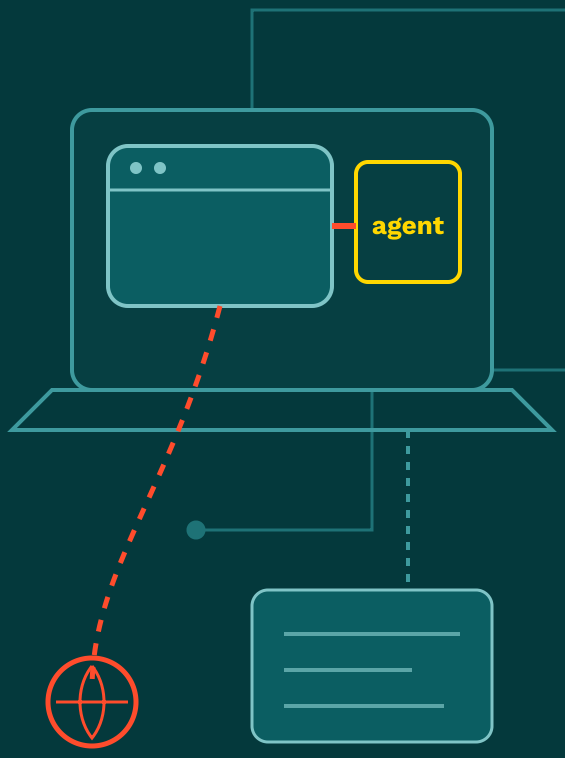
CASE STUDY

CS-2026-05

ioSENTRIX

Your Trusted Partner in Cybersecurity



APPLICATION AND DESKTOP AGENT SECURITY

How any website could take control of a company's desktop agent

An open local connection and a token in memory exposed data across the whole platform.

CLIENT
Technology company

SERVICE
Web, API and desktop agent penetration testing

ENGAGEMENT
Multi-week engagement

VERIFIED
All findings closed; retested by ioSENTRIX

AT A GLANCE

CLIENT
Technology company

PRODUCT
Web platform with a desktop agent for staff

SERVICE
Thick client and desktop application testing

SCOPE
Web application, backend APIs and the desktop agent

ENGAGEMENT
A multi-week engagement

VERIFIED
All findings closed; retested by ioSENTRIX

TESTED BY
ioSENTRIX application and thick-client testers

EXECUTIVE SUMMARY

Any website could reach the desktop agent, and one stolen token could reach data across the platform

A technology company asked ioSENTRIX to test its web application, its backend APIs and the desktop agent its staff install.

We found that any website a user visited could control the agent through an unprotected local connection, and that a token read from memory bypassed device registration and opened data across the whole platform. The client closed every finding, and ioSENTRIX retested the fixes.

10+	1	2
findings across web, API and desktop	Critical: any website could drive the agent	attack chains, one reaching platform-wide data

A token copied from memory walked straight around device registration.

Details in this case study are anonymised and generalised. Methods that could harm other products are withheld.

© 2026 ioSENTRIX LLC

01 What we found

CRITICAL FINDING 1

Any website could control the desktop agent

The agent ran a local WebSocket server with no encryption, authentication or origin check. Any web page open in the user's browser could connect and call sensitive agent functions and even make the machine scan the internal network.

Business impact: a malicious website could use the agent, and its reach into the internal network, on any staff machine with no user interaction.

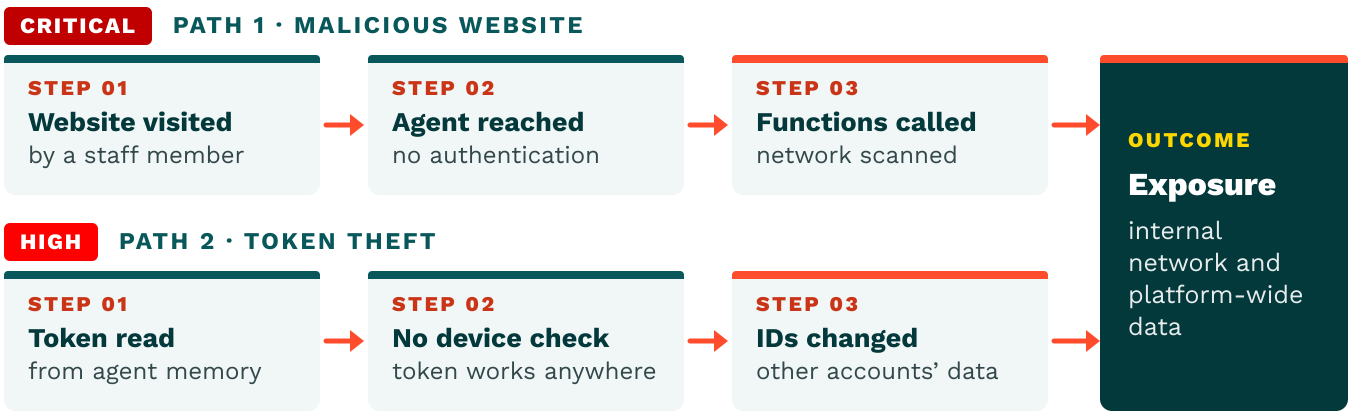
HIGH FINDING 2

A token in memory beat device registration

The agent kept its sign-in token in plain text in memory, readable with standard tools and no admin rights. The token worked from any machine, defeating device registration, and missing ownership checks on the APIs let it open other accounts' records and customer details.

Business impact: one compromised workstation could expose data across the entire platform.

Figure 1. Two paths from a single staff machine to platform-wide exposure



HOW WE FOUND IT

Desktop agents fall between web and endpoint testing, so neither a web scanner nor an endpoint tool looks at the local connection between them. Finding this took testing the agent, the browser and the APIs together.

© 2026 ioSENTRIX LLC

02 Results

Figure 2. Findings by severity (10+ findings)[1]



Also found: a hard-coded database password in the agent, server-side request forgery, missing cookie flags, a password-change endpoint open to brute force, an outdated library and weak TLS ciphers.

WHAT CHANGED

All closed by the client; retested by ioSENTRIX

- **Agent connection.** Encrypted, authenticated and origin-checked.
- **APIs.** Ownership checked on every object, from the session, not the request.
- **Tokens.** Protected in memory with platform encryption and cleared after use.
- **Hygiene.** Hard-coded credentials removed, rate limits added, libraries upgraded.

03 Lessons for product teams

A local server is a public server

Any website can reach localhost unless you authenticate and check origin.

Device binding needs protected tokens

If a token can be copied, the device check can be skipped.

Check ownership on every object

The ID in a request is the user's claim, not proof (OWASP API1).[2]

[1] Severity rated on a five-level likelihood and impact matrix based on NIST SP 800-30 Rev. 1.

[2] OWASP API Security Top 10 (2023): API1 Broken Object Level Authorization, API5 Broken Function Level Authorization. Cited as alignment guidance.

ioSENTRIX

Shipping a desktop agent or companion app? See a sample thick-client test report or book a strategy session.

iosentrix.com/contact-us

contact@iosentrix.com

+1 (888) 958-0554

13800 Coppermine Rd, Suite 190
Herndon, VA 20171

CREST-accredited · ISO/IEC 27001 certified · SOC 2 Type 2 attested

© 2026 ioSENTRIX LLC. General information only. Client details anonymised.