EXPOSURE STUDY

ULTRARED

EXPOSURE RISKS IN THE INSURANCE SECTOR: A REAL-WORLD CASE STUDY

Executive Summary

Insurance organizations are accelerating digital transformation: expanding customer portals, claims systems, agent applications, and cloud environments. But this modernization introduces risk exposures that traditional scanners rarely detect.

In a recent assessment of a major global insurance provider, ULTRA RED uncovered a critical exposure chain combining **Broken Access Control** with **Exposed AWS Cognito Credentials.** This allowed attackers to generate valid OAuth tokens, bypass authentication, and gain unrestricted access to sensitive internal APIs, including customer communications, policy data, and voice records.

This case underscores a broader industry risk: in the insurance sector, identity misconfigurations and cloud credential leaks can silently open the door to a full-system compromise.

Overview of Threats Targeting Insurance Organizations

Rising Value of Insurance Data

Insurers store rich personal, financial, medical, and behavioral data, making them prime targets for fraud, extortion, and identity theft.

Fragmented Subsidiaries & Broker Networks

Multiple brands, agents, and regional platforms increase the attack surface and create security blindposts.

API-Driven Digital Workflows

Customer self-service, claims automation, and policy management rely heavily on APIs, making misconfigurations a top path to compromise.

Legacy Meets Cloud

Older portals, third-party integrations, and new cloud-native apps coexist, creating blind spots and identity drift.

Exposed Non-Production Assets

Staging and QA environments often contain real credentials, creating critical exposure risk.

Third-Party & Vendor Integrations

Insurance platforms rely heavily on external vendors, which expands the attack surface and introduces shared risk.

Real-World Example: Full Compromise Through Broken Access Control & Exposed Cloud Credentials

During routine external scans, ULTRA RED identified two severe vulnerabilities within a large insurance provider's digital ecosystem.

When combined, these weaknesses granted full unauthorized access to internal backend systems.

1 Exposed AWS Cognito OAuth Credentials

A public-facing JavaScript file embedded hard-coded **AWS Cognito client_id and client_secret.** Anyone could use these credentials to request valid OAuth tokens directly from the cloud authentication service.
This meant attackers could instantly impersonate trusted application components and obtain legitimate access tokens, with no login required.

2 Broken Access Control Across Internal APIs

Backend APIs fully trusted any presented token without verifying user roles, privileges, or the legitimacy of the client. Once an attacker acquired a token using the exposed credentials, the system applied no authorization checks.

This enabled direct, unrestricted access to high-sensitivity endpoints, including:

- Internal and external email search
- Full email message content
- Chat and conversation data
- IVR and voice-recording systems
- Endpoints capable of modifying or deleting information

This was not a theoretical chain – ULTRA RED validated end-to-end exploitability of this exposure using real attacker workflows.

The Impact

With only two misconfigurations, a remote attacker could:

- Retrieved sensitive customer and employee communications
- Extracted PII, policy details, and operational data
- Altered records or disrupted claims workflows
- Impersonated internal systems or support portals
- Triggered major regulatory violations (GDPR, Solvency II)

For an insurance provider, this exposure represented a complete **backend compromise.**

Conclusion:
How Insurance Providers Can Protect Against These Exposures

Enforce Strong Server-Side Authorization
Every API call must validate user identity, role, and permissions – never trust tokens blindly.

Remove Secrets From Frontend Code
Cloud credentials, OAuth secrets, and API keys should never appear in public JavaScript or mobile applications.

Secure Token Issuance Endpoints
Restrict token creation through origin controls, mTLS, OAuth scopes, and IP allowlists.

Continuously Validate Exploitability
Surface-level scanning isn't enough. Organizations must know which exposures can be weaponized.

Monitor Cloud Identity Drift
Misconfigured identity providers, permissive roles, and unused secrets are among the most dangerous risks in modern insurance ecosystems.

Limit Third-Party and Partner Access by Design
Apply least-privilege access to partners, brokers, and service integrations, and continuously validate what external systems can actually reach.

How ULTRA RED Helps

ULTRA RED's **validation-first CTEM platform** continuously discovers all externally exposed assets across insurance subsidiaries, brands, cloud workloads, and partner environments. The platform automatically validates every exposure end-to-end, proving exploitability with real attacker-level evidence.

With zero false positives, ULTRA RED enables security teams to confidently prioritize and remediate identity, API, and cloud misconfigurations, closing the hidden gaps that can lead to compromises.

About ULTRA RED

ULTRA RED is a pioneer and leading provider of Continuous Threat Exposure Management (CTEM) solutions, built on a validation-first approach. Our CTEM platform helps security teams confidently reduce threat exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface. Learn more at www.ultrared.ai.