INDUSTRY CASE STUDY

ULTRARED

SECURING TELECOM'S EXPANDING ATTACK SURFACE

Executive Summary

Telecom companies are under growing pressure to secure vast, complex, and increasingly AI-targeted attack surfaces — from legacy infrastructure to cloud assets and shadow environments. Recently, ULTRA RED uncovered a critical authorization flaw in a European telecom provider's internal portal, exposing more than 11,000 devices to potential unauthorized takeover.

This case highlights a broader industry risk: traditional vulnerability scanning alone is no longer enough. **ULTRA RED's validation-first CTEM platform** helps telecom organizations discover exposed assets, automatically validate exploitability, and remediate faster — all with fewer than 1% false positives. In a sector where outages or breaches can have critical impact, proactive exposure validation is essential.

Background: Telecom's Shifting Threat Landscape

Telecommunications companies are the digital arteries of modern society — responsible not only for communication but also for supporting entire economies, critical infrastructure, and increasingly, IoT ecosystems. But this centrality comes at a cost: the telecom industry is under constant threat.

Unlike other sectors, telecom firms manage vast, decentralized infrastructures with millions of exposed devices, public-facing portals, legacy systems, and third-party dependencies. The complexity, scale, and criticality of telecom networks make them an ideal target for attackers — and a big challenge for security teams.

With the rise of AI-powered attacks, those challenges are only intensifying — enabling adversaries to discover vulnerabilities faster, launch automated campaigns at scale, and bypass traditional defenses with greater precision.

Unique Exposure Risks in Telecom

Telecom providers face several challenges that make them uniquely vulnerable:

Massive Attack Surfaces

Public-facing management portals, mobile applications, and exposed APIs are common across telecom environments.

Legacy Infrastructure

Outdated technologies and inconsistent patching across infrastructure and consumer equipment often lead to exploitable blind spots.

Device-Heavy Environments

Telecom fleets include thousands of remotely managed phones, routers, and IoT devices — each a potential entry point for adversaries.

Complex Authentication Flows

Fragmented and sometimes insecure access controls across user and admin portals create prime conditions for privilege escalation or bypasses.

Real-World Case: Critical Authorization Bypass in a Telecom Portal

ULTRA RED's automated CTEM platform and research team recently uncovered a **critical authorization flaw** in the internal device management portal of a leading European telecom provider. This discovery exposed a deeply rooted architectural vulnerability — one that granted unauthenticated access to highly sensitive infrastructure.

Discovery

During scans, our team identified that login enforcement relied entirely on client-side JavaScript redirects. By intercepting and removing this JavaScript, we bypassed authentication and accessed the admin panel — no credentials required. Backend APIs lacked any server-side access control.

What Was Exploited

Client-side authentication logic — easily removed to gain access.

Unprotected backend endpoints — accessible without login or session validation.

What We Found

By manipulating client-side responses, we bypassed login protections and gained unauthorized access to the company's **Telephone Management Panel,** revealing a staggering level of control:

Full control of 11,649 remotely managed phones — including reboot, firmware updates, and configuration changes.

Downloadable ROMs — potentially usable for reverse engineering or malware injection.

Firmware push capability — enabling mass compromise or device bricking.

CSV and XML import tools — opening the door to silent data corruption or even remote code execution.

Sensitive metadata — including IP addresses, phone numbers, and device IDs.

Root Cause

Authentication was enforced only via client-side JavaScript, while backend APIs remained unprotected — an architectural flaw ripe for exploitation.

The Risk

This wasn't just a theoretical risk. A threat actor exploiting this flaw could have crippled thousands of devices, manipulated telecom traffic, or launched large-scale surveillance campaigns — all without alerting a single security system.

The Broader Threat Landscape

While this case involved one telecom provider, similar vulnerabilities pose risk across the telecom sector:

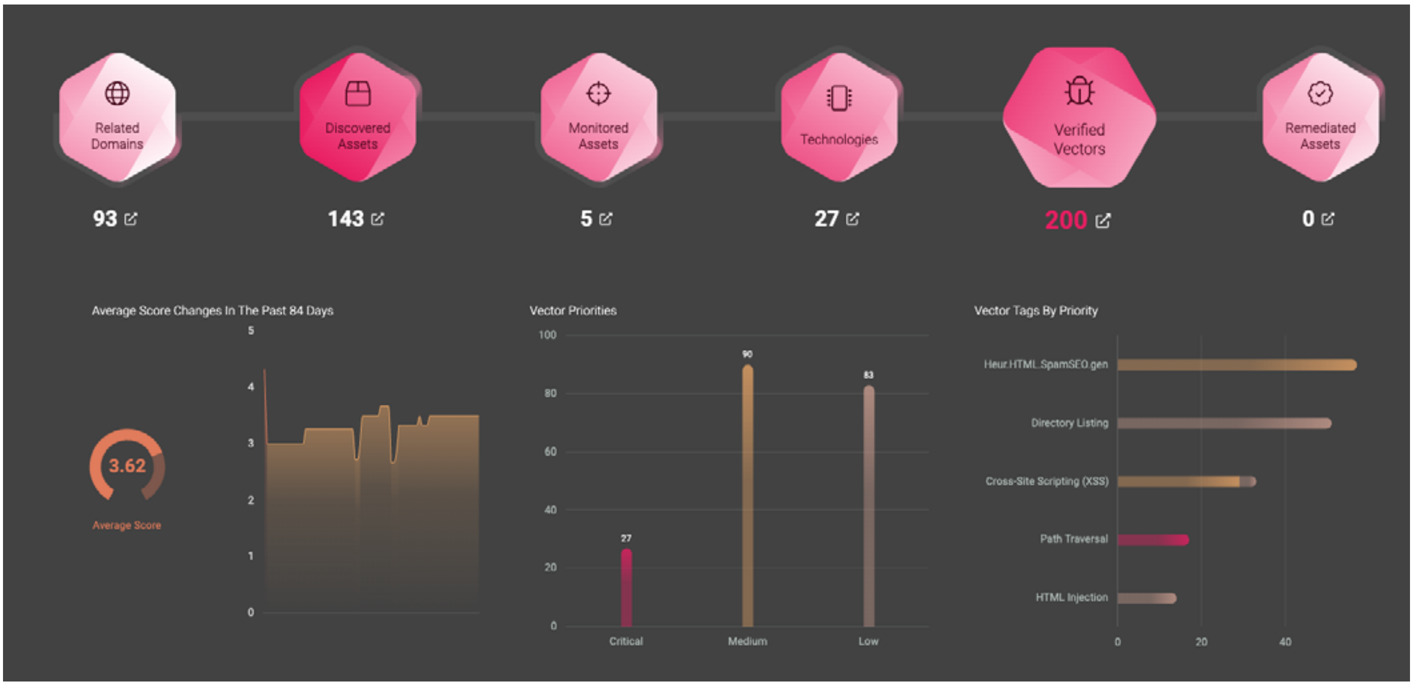
- **Misconfigured device portals** exposing control panels online
- **Overlooked dev environments** left accessible post-launch
- **Unauthenticated APIs** in mobile apps and customer service platforms
- **Third-party integrations** that introduce shadow IT risks

In an era of 5G, VoIP, and eSIM provisioning, the risks only multiply. Telecom companies need to go beyond detecting vulnerabilities — and start validating exposures.

How ULTRA RED Helps

ULTRA RED's validation-first CTEM platform empowers telecom companies to confidently manage and reduce their threat exposure — even across complex, legacy-heavy infrastructures. The agentless solution continuously discovers all externally facing assets, automatically validates 100% of exposures with proof of exploitability, and delivers clear remediation guidance.

With fewer than 1% false positives, security teams can trust the findings, focus on real threats, and respond faster — without second-guessing every alert.



ULTRA RED enables you to:

Discover exposed assets across subsidiaries, third parties, and shadow environments.

Automatically validate exploitability with real-world evidence.

Continuously scan the external attack surface from an attacker's perspective — uncovering potential entry points.

Remediate faster using AI-powered guidance — closing exposures before they escalate.

Protect Your Telecom Operations

Telecom providers can no longer rely on surface-level scanning or reactive patching. When entire device fleets, customer data, and national infrastructure are on the line, **proactive exposure validation** is non-negotiable.

Ready to discover and validate your true attack surface?

Get a Free Exposure Assessment from ULTRA RED.

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. Founded in 2021, the company is headquartered in Tel Aviv, Israel. Learn more at **www.ultrared.ai.**