



EXTERNAL PERIMETER ASSESSMENT · LARGE COMMUNICATIONS GROUP

A sprawling external perimeter, held open by default passwords

A large telecommunications group with a broad, recently expanded perimeter

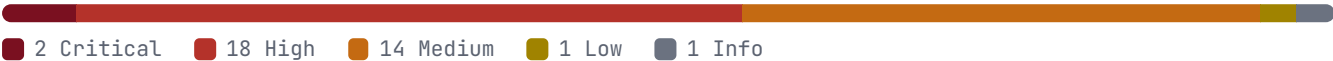
Anonymized with the client's written permission. The organization, systems, hostnames, addresses, accounts and other identifiers in the original report have been removed or generalized. Findings are described at a level that cannot be traced back to the client.

Client	A large communications group (anonymized)
Engagement	External network penetration test across a wide internet-facing estate
Approach	Black-box external testing with non-invasive exploitation, roughly two weeks
Tester	Ismail Regragui, Vallum Security · OSCP, OSEP, BSCP, OSWP · Synack Red Team
Standards	NIST SP 800-115, OWASP Testing Guide v4.2; severity by CVSS v4.0

What we were asked to do

Measure the external attack surface of a large, fast-growing estate, much of it recently absorbed through acquisitions, and show which internet-facing systems an attacker could take over without any prior access.

Results at a glance



Findings at a glance

ID	FINDING	SEVERITY
1	Administrative access to network and IoT devices via default or blank credentials (multiple devices)	Critical
2	Anonymous file and remote-shell access to network devices	Critical

3	Directory traversal exposing sensitive configuration and credentials	High
4	Admin access to video, telematics and EV-charging management dashboards via default credentials	High
5	Credential disclosure and authentication bypass on consumer-grade routers	High
6	Known remote-code-execution flaws in outdated embedded web servers and network software	High
7	Plaintext credentials and secrets exposed in application responses and config files	High
8	Exposed monitoring dashboards and time-series databases without authentication	Medium
9	Exposed CI/build server allowing unauthenticated file read	Medium
10	Anonymous and null-session file-share access leaking system information	Medium
11	Account enumeration on mail and remote-access services	Medium
12	Sensitive data passed in URLs, and other information-disclosure issues	Medium
13	Valid corporate credentials recovered from open-source breach data (OSINT)	Info

The original report contained 36 findings across many systems. They are grouped and retitled here by theme. All device models, hostnames, addresses, subnets and credentials have been removed.

The pattern: two weaknesses, repeated across the estate

Rather than one deep chain, the engagement found the same two weaknesses again and again across a very large perimeter.

- 1. Default credentials.** Many internet-facing devices, from routers to specialized appliances, were reachable with factory or blank credentials, giving administrative control with no real effort.
- 2. Weak patching.** Large numbers of hosts ran years-old software with public exploits, including unauthenticated information-disclosure and remote-code-execution flaws.
- 3. Exposed services.** Monitoring dashboards, databases and build servers sat on the open internet without authentication, leaking internal data and, in places, plaintext credentials.
- 4. Open-source intelligence.** Before any testing, valid corporate credentials were recovered from public breach data, a ready foothold for an attacker.
- 5. Breadth over depth.** With the client's agreement, invasive exploitation was held back: the point was shown by the sheer number of soft targets, not by pushing any single one to full compromise.

The estate was uneven: some segments were well defended, with firewalls, IP bans and automatic shutdown of compromised services, which is noted in the strengths below.

What was working

- ✓ Some segments blocked common scanning tools and detected enumeration attempts.
- ✓ Several compromised services shut themselves down automatically, preventing re-access.
- ✓ Parts of the network showed effective segmentation, with updated components and strong passwords, limiting an attacker's reach.

Remediation themes

- Eliminate default and blank credentials across all internet-facing devices, and remove or firewall services that do not need to be public.
- Establish asset inventory and patch management for the full perimeter, especially for recently acquired estates.
- Move monitoring, database, build and admin interfaces behind VPN or authentication, and never expose them directly.
- Rotate any credentials found in public breach data, and roll out multi-factor authentication on external services.

Outcome. The client received a prioritized view of its external exposure across a large, growing estate, with a clear first wave of fixes (default credentials and exposed admin services) and a recommendation to retest the perimeter regularly.