Idrak Security

CONFIDENTIAL

External Security Assessment — Larémont Group S.r.l.

Client	Larémont Group S.r.l.
Project	Valutazione esposizione esterna Q1 2026
Report Date	2026-07-30
Test Period	2026-07-20 — 2026-07-24
Lead Analyst	Idrak Security Team
Version	1.0

SECTION 00

Indice

SECTION 01

Executive Summary

Idrak Security ha condotto una valutazione della superficie di attacco esterna di Larémont Group S.r.l., realtà operante nel settore e-commerce per l'arredamento e il design. L'attività ha simulato le fasi di ricognizione e accesso iniziale di un potenziale attaccante, operando esclusivamente su fonti pubbliche e nel perimetro definito dalle Rules of Engagement sottoscritte dal cliente.

L'analisi ha identificato quattro vulnerabilità: una di criticità alta, due medie e una bassa. La principale criticità riguarda un pannello di amministrazione esposto pubblicamente in assenza di restrizioni di accesso. La postura di sicurezza esterna è stata valutata a rischio medio. Le vulnerabilità riscontrate sono risolvibili in tempi brevi e i relativi interventi tecnici sono elencati nel report in ordine di priorità.

VULNERABILITY SUMMARY

1	3
High	Medium

SECTION 02

Project Information

Organizzazione: Larémont Group S.r.l., Corso Vittorio Emanuele II 45, 10128 Torino (TO)

Nome Progetto: Valutazione dell'esposizione esterna Q1 2026

Tipo di Assessment: Ricognizione esterna passiva e verifica manuale limitata su perimetro autorizzato

Periodo di Esecuzione: dal 20 luglio 2026 al 24 luglio 2026

Analista Responsabile: Marco Rossi

SECTION 03

Scope

Tutte le attività sono state condotte nel rispetto delle Rules of Engagement formalmente approvate e sottoscritte dal cliente prima dell'inizio delle attività.

Asset in ambito:

https://laremont-group.it/ — Applicazione Web — Sito e-commerce principale

https://shop.laremont-group.it/ — Applicazione Web — Piattaforma di vendita

https://admin.laremont-group.it/ — Pannello amministrativo — Accesso gestionale

Caselle email pubbliche e PEC — Email — Superficie di phishing e spoofing

SECTION 04

Methodology

Analisi della superficie di attacco (Attack Surface Analysis)

Verifica della superficie esposta (Exposure Check)

Scansione delle vulnerabilità (Vulnerability Scanning)

Verifica di conformità (articoli 32 e 5 del GDPR)

Valutazione dell'impatto del rischio

SECTION 05

Attack Surface

admin.laremont-group.it — Pannello amministrativo — Esposizione pubblica — Rischio alto

shop.laremont-group.it — Piattaforma e-commerce — Esposizione pubblica — Rischio medio

Record SPF e DMARC del dominio — Configurazione email — Esposizione pubblica — Rischio medio

Certificato SSL sito principale — Configurazione TLS — Esposizione pubblica — Rischio basso

SECTION 06

Vulnerability Summary

Pannello di amministrazione esposto pubblicamente — Alta — admin.laremont-group.it — Rischio di accesso non autorizzato al gestionale e ai dati clienti

Configurazione SPF e DMARC assente o permissiva — Media — Dominio email — Rischio di spoofing e phishing a nome dell'azienda

Intestazioni HTTP rivelano versioni software — Media — shop.laremont-group.it — Agevolazione di attacchi mirati basati su vulnerabilità note

Certificato SSL in scadenza — Bassa — laremont-group.it — Possibile interruzione dell'accesso sicuro e perdita di fiducia degli utenti

SECTION 07

Attack Path

00:00 — Reconnaissance e mappatura dei sottodomini

00:30 — Identificazione del pannello di amministrazione esposto

01:00 — Verifica delle configurazioni email e DNS

01:20 — Analisi della validità e configurazione del certificato SSL

01:40 — Consolidamento delle evidenze raccolte

SECTION 08

Findings

Vulnerabilità 1

Titolo: Esposizione pubblica del pannello di amministrazione privo di restrizioni d'accesso

Asset interessato: admin.laremont-group.it

Livello di gravità: Alto

Descrizione tecnica: L’interfaccia di amministrazione risulta accessibile pubblicamente da qualsiasi indirizzo IP, in assenza di restrizioni perimetrali e di autenticazione a più fattori (MFA). La pagina di login è indicizzata dai motori di ricerca e accessibile direttamente.

Modalità di sfruttamento: Un malintenzionato può condurre attacchi di tipo brute force o credential stuffing sul portale di accesso, oppure tentare l’exploit di vulnerabilità note del CMS per acquisire privilegi amministrativi.

Impatto potenziale: Accesso non autorizzato alla piattaforma gestionale, con conseguente manipolazione degli ordini, esfiltrazione dell’anagrafica clienti e alterazione dei contenuti del sito.

Raccomandazione: Limitare l'accesso al pannello tramite whitelist IP o VPN, implementare l'autenticazione a due fattori e rimuovere la pagina dall'indicizzazione dei motori di ricerca.

Vulnerabilità 2

Vulnerabilità 2

Titolo: Configurazioni SPF e DMARC assenti o permissive

Asset interessato: Dominio email laremont-group.it

Livello di gravità: Medio

Descrizione tecnica: Il dominio non dispone di un record DMARC e il record SPF è configurato con policy permissiva. Tale scenario consente lo spoofing dell'identità e-mail aziendale.

Modalità di sfruttamento: Un attaccante può inviare comunicazioni di phishing spacciandole per comunicazioni legittime dell'azienda, inducendo in errore clienti e personale interno.

Impatto potenziale: Esecuzione di campagne di phishing a nome dell'organizzazione, frodi ai danni dei clienti e compromissione della reputazione aziendale.

Raccomandazione: Implementare un record DMARC in modalità "reject", ottimizzare il record SPF e configurare il protocollo DKIM.

Vulnerabilità 3

Titolo: Esposizione delle versioni software tramite intestazioni HTTP

Asset interessato: shop.laremont-group.it

Livello di gravità: Medio

Descrizione tecnica: Le risposte HTTP del server rivelano le versioni specifiche del web server e del framework applicativo attraverso gli header "Server" e "X-Powered-By".

Modalità di sfruttamento: Queste informazioni consentono a un utente malintenzionato di identificare vulnerabilità note (CVE) relative alle versioni in uso e di pianificare attacchi mirati.

Impatto potenziale: Riduzione dei tempi di ricognizione per l'attaccante e incremento della probabilità di successo di un tentativo di intrusione.

Raccomandazione: Rimuovere o offuscare le intestazioni "Server" e "X-Powered-By" all'interno della configurazione del web server.

Vulnerabilità 4

Titolo: Certificato SSL in scadenza imminente

Asset interessato: laremont-group.it

Livello di gravità: Basso

Descrizione tecnica: Il certificato SSL associato al dominio principale scadrà entro 21 giorni. La scadenza del certificato compromette la navigazione sicura e genera avvisi di sicurezza per i visitatori.

Modalità di sfruttamento: Non direttamente sfruttabile per un attacco, tuttavia la scadenza causa l'interruzione del servizio e una perdita di fiducia da parte degli utenti.

Impatto potenziale: Indisponibilità dell'accesso sicuro al sito, potenziale calo delle vendite e visualizzazione di errori di sicurezza agli utenti finali.

Raccomandazione: Provvedere al rinnovo del certificato SSL prima della data di scadenza e configurare sistemi di rinnovo automatico.

SECTION 09

Exploit

Prova 1. Richiesta normale

Comando: curl -I https://admin.laremont-group.it/

Risposta: HTTP/1.1 200 OK, pagina di login accessibile senza restrizione IP.

Prova 2. Verifica record DMARC

Comando: dig TXT _dmarc.laremont-group.it

Risposta: nessun record DMARC presente.

Prova 3. Intestazioni server

Comando: curl -I https://shop.laremont-group.it/

Risposta: Server: Apache/2.4.29, X-Powered-By: PHP/7.2.10

Prova 4. Scadenza certificato

Verifica: il certificato SSL di laremont-group.it risulta valido fino a 21 giorni dalla data del test.

SECTION 10

Impact

Rischio Economico: Medio. In caso di sfruttamento, l'azienda potrebbe sostenere costi di gestione dell'incidente, ripristino dei sistemi e interruzione delle vendite online.

Rischio Reputazionale: Medio-alto. Un accesso non autorizzato ai dati dei clienti di un e-commerce comprometterebbe la fiducia degli acquirenti.

Rischio Compliance GDPR: Alto. L'esposizione del pannello amministrativo e la configurazione email carente possono determinare una violazione degli articoli 5 e 32 del GDPR relativi a integrità, riservatezza e sicurezza del trattamento.

Rischio Interruzione Operativa: Medio. Le vulnerabilità rilevate potrebbero essere sfruttate per alterare le pagine o interrompere il servizio di vendita.

SECTION 11

Recommendations

Priorità 1: Restringere immediatamente l'accesso al pannello amministrativo tramite whitelist IP e autenticazione a due fattori.

Priorità 2: Implementare DMARC in modalità reject e correggere SPF e DKIM.

Priorità 3: Rimuovere le intestazioni server che rivelano le versioni software.

Priorità 4: Rinnovare il certificato SSL e attivare il rinnovo automatico.

SECTION 12

Scorecard

Punteggio complessivo: 62 su 100

Sicurezza dell'infrastruttura: 65 su 100, rischio medio

Sicurezza email: 55 su 100, rischio medio

Sicurezza applicativa: 48 su 100, rischio alto

Protezione dei dati: 68 su 100, rischio medio

Configurazione TLS: 80 su 100, rischio basso

SECTION 13

Appendix

Riferimenti normativi: Regolamento UE 2016/679 (GDPR), articoli 5 e 32. Direttiva UE 2022/2555 (NIS2), recepita in Italia con D.Lgs. 138/2024, articolo 21.

Metodologia di riferimento: OWASP Testing Guide, OSSTMM.

Glossario: SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication), DKIM (DomainKeys Identified Mail), TLS (Transport Layer Security), CMS (Content Management System).

Disclaimer: il presente report riflette lo stato dei sistemi alla data del test. Idrak Security ha operato esclusivamente nell'ambito autorizzato dalle Rules of Engagement sottoscritte dal cliente.

SECTION 14

Technical Findings

`64541e89` **Esposizione pubblica del pannello di amministrazione privo di restrizioni d'accesso** — High

ASSET

`admin.laremont-group.it`

DESCRIPTION

L'interfaccia di amministrazione risulta accessibile pubblicamente da qualsiasi indirizzo IP, in assenza di restrizioni perimetrali e di autenticazione a più fattori. La pagina di login è indicizzata dai motori di ricerca e accessibile direttamente.

EXPLOITATION

Un attaccante può condurre attacchi di forza bruta o credential stuffing sul portale di accesso, oppure sfruttare vulnerabilità note del CMS per acquisire privilegi amministrativi.

IMPACT

Accesso non autorizzato alla piattaforma gestionale, con manipolazione degli ordini, esfiltrazione dell'anagrafica clienti e alterazione dei contenuti del sito.

RECOMMENDATION

Limitare l'accesso al pannello tramite whitelist IP o VPN, implementare l'autenticazione a due fattori e rimuovere la pagina dall'indicizzazione dei motori di ricerca.

Nota di Conformità: GDPR Art. 32, NIS2 Art. 21

`a59d5770` **Configurazione SPF e DMARC assente o permissiva** — Medium

`c6ad3bdb` **Esposizione delle versioni software tramite intestazioni HTTP** — Medium

`0eba0c0e` **Certificato SSL in scadenza imminente** — Medium

SECTION 15

Evidenze e Screenshot

Le seguenti evidenze sono state raccolte durante l'attività di assessment.

SECTION 16

Conclusioni

La valutazione ha individuato criticità concrete, in particolare l'esposizione pubblica del pannello amministrativo, che rappresenta il rischio più rilevante. Le altre vulnerabilità riguardano la configurazione email, le intestazioni server e il certificato SSL. Tutte sono correggibili in tempi brevi. Si raccomanda di intervenire con priorità sul pannello amministrativo e di avviare un rafforzamento strutturato delle misure di sicurezza per garantire aderenza ai requisiti del GDPR e della direttiva NIS2.

SECTION A

Appendice — Metodologia e Classificazione

Metodologia di Valutazione

L'assessment è stato condotto seguendo le metodologie OWASP Testing Guide v4.2 e PTES (Penetration Testing Execution Standard).

Classificazione della Severità

Critical Vulnerabilità che consente l'accesso non autorizzato completo al sistema. Richiede intervento immediato.

High Vulnerabilità che consente accesso parziale non autorizzato. Remediation entro 7 giorni.

Medium Vulnerabilità sfruttabile in combinazione con altre. Remediation entro 30 giorni.

Low Vulnerabilità a basso impatto. Remediation entro 90 giorni.

Disclaimer

I risultati presentati riflettono lo stato di sicurezza al momento dell'assessment. Idrak Security declina ogni responsabilità per modifiche successive.