NullTrace

RISERVATO

VULNERABILITY ASSESSMENT ESTERNO · ESSENZIALE · TECHNOLOGY & CVE REPORT

Sai davvero cosa utilizza il tuo sito?

aziendatest.example

ESEMPIO · DATI FITTIZI

CLIENTE	PERIODO DELL'ANALISI	CONSEGNA
Azienda Test (fittizia)	10/11/2026 → 12/11/2026	13/11/2026
PERIMETRO	**LIVELLO**	**ID REPORT**
3 indirizzi	Essenziale	NT-ESEMPIO-ESSENZIALE

OSSERVAZIONI PER GRAVITÀ · 7 IN TUTTO



1 critico **4** alto **2** medio

ESEMPIO

Questo è un esempio con dati fittizi. Il report che riceverai ha la stessa struttura, ma può essere più o meno ricco a seconda di ciò che emerge sul tuo sito.

01 Sintesi

12
tecnologie rilevate

7
obsolete o senza supporto

7
CVE potenzialmente pertinenti

Il sito usa diversi componenti non aggiornati. Il punto più urgente è il plugin del modulo contatti, in una versione con una falla critica nota. PHP e MySQL non ricevono più correzioni dal produttore. Le CVE sono dedotte dalle versioni dichiarate: vanno confermate con il fornitore, che a volte applica le correzioni senza cambiare il numero di versione.

02 Tecnologie rilevate

CATEGORIA	TECNOLOGIA	VERSIONE	STATO	DOVE SI VEDE
Server web	**nginx**	1.18.0	OBSOLETA	header Server
Sistema operativo	**Ubuntu**	22.04 LTS	SUPPORTATA	banner SSH e header
Linguaggio	**PHP**	7.4.33	SENZA SUPPORTO	header X-Powered-By
CMS	**WordPress**	6.1.1	OBSOLETA	meta generator
Plugin	**Contact Form 7**	5.3.1	OBSOLETA	file del plugin (?ver=)
Plugin	**Yoast SEO**	20.1	OBSOLETA	commento nel codice HTML
Libreria JavaScript	**jQuery**	1.12.4	OBSOLETA	file della libreria (?ver=)
Database	**MySQL**	8.0.28	SENZA SUPPORTO	porta 3306
Accesso remoto	**OpenSSH**	8.9p1	DA VERIFICARE	porta 22
Certificato HTTPS	**Let's Encrypt**	–	VALIDO	valido fino al 20/01/2027
Statistiche	**Google Analytics 4**	–	SERVIZIO ESTERNO	script nella pagina
Newsletter	**Mailchimp**	–	SERVIZIO ESTERNO	modulo di iscrizione

03 Osservazioni

Dalla più grave. «Potenziale» vuol dire dedotta dalla versione dichiarata, da confermare con il fornitore.

CRITICO POTENZIALE Contact Form 7 5.3.1 F-01

Il modulo contatti usa una versione con una falla critica nota

COSA SIGNIFICA La versione del plugin del modulo contatti è tra quelle in cui si potevano caricare file pericolosi sul sito.

COSA FARE Aggiorna Contact Form 7 all'ultima versione dal pannello di WordPress. La falla è corretta dalla 5.3.2 in poi.

CVE-2020-35489 · CVSS 10.0

ESEMPIO · DATI FITTIZI

ALTO OSSERVATO PHP 7.4.33 F-02

PHP 7.4 non riceve aggiornamenti di sicurezza da novembre 2022

COSA SIGNIFICA Il linguaggio su cui gira il sito non viene più corretto: le falle scoperte dopo il 2022 restano aperte.

COSA FARE Chiedi al fornitore dell'hosting di passare a PHP 8.3 o 8.4, dopo una prova sul sito di test.

ALTO OSSERVATO MySQL 8.0.28 F-03

MySQL 8.0 non riceve più aggiornamenti da aprile 2026

COSA SIGNIFICA Il database del sito usa una versione che il produttore non corregge più.

COSA FARE Pianifica con il fornitore il passaggio a MySQL 8.4, la versione con supporto a lungo termine.

ALTO POTENZIALE OpenSSH 8.9p1 (Ubuntu) F-04

OpenSSH dichiara una versione colpita da una falla nota

COSA SIGNIFICA La versione dell'accesso remoto al server rientra tra quelle colpite, se il fornitore non ha applicato la correzione.

COSA FARE Chiedi al fornitore di aggiornare i pacchetti del server: Ubuntu ha corretto la falla anche sulla 22.04.

CVE-2024-6387 · CVSS 8.1

ALTO POTENZIALE nginx 1.18.0 (Ubuntu) F-05

nginx 1.18.0 rientra in una falla nota del resolver DNS

COSA SIGNIFICA La versione del server web è colpita solo se usa la funzione interna di risoluzione DNS: va verificato.

COSA FARE Aggiorna nginx con i pacchetti della distribuzione e controlla se la configurazione usa la direttiva resolver.

CVE-2021-23017 · CVSS 7.7

MEDIO POTENZIALE WordPress 6.1.1 F-06

WordPress 6.1.1 è indietro di molte versioni

COSA SIGNIFICA Il programma che gestisce il sito non è aggiornato e include almeno una falla nota, corretta da tempo.

COSA FARE Aggiorna WordPress all'ultima versione dal pannello, dopo un backup e una prova sul sito di test.

CVE-2023-2745 · CVSS 6.1

MEDIO POTENZIALE jQuery 1.12.4 F-07

La libreria jQuery 1.12.4 ha tre falle note

COSA SIGNIFICA Una libreria usata dalle pagine ha falle note che, in certi casi, permettono di inserire codice nella pagina.

COSA FARE Aggiorna il tema e i plugin che la caricano: le versioni recenti usano jQuery 3.5 o successive.

CVE-2019-11358 · CVSS 6.1 CVE-2020-11022 · CVSS 6.1 CVE-2020-11023 · CVSS 6.1

ESEMPIO · DATI FITTIZI

04 Falle note (CVE) potenzialmente pertinenti

Dedotte dalle versioni dichiarate: non sono vulnerabilità confermate. Punteggi CVSS da NVD.

COMPONENTE	CVE	CVSS	COSA RIGUARDA	CORRETTA IN
Contact Form 7 5.3.1	CVE-2020-35489	10.0	Caricamento di file pericolosi tramite il modulo	5.3.2
OpenSSH 8.9p1 (Ubuntu)	CVE-2024-6387	8.1	Accesso remoto senza password, in condizioni particolari	Ubuntu USN-6859-1
nginx 1.18.0	CVE-2021-23017	7.7	Errore di memoria nel resolver DNS interno	1.20.1
WordPress 6.1.1	CVE-2023-2745	6.1	Caricamento di file di traduzione arbitrari	6.2.1
jQuery 1.12.4	CVE-2019-11358	6.1	Modifica degli oggetti JavaScript (prototype pollution)	3.4.0
	CVE-2020-11022	6.1	Esecuzione di codice da HTML non fidato	3.5.0
	CVE-2020-11023	6.1	Esecuzione di codice da HTML con elementi option	3.5.0

05 In breve

- Yoast SEO 20.1 è indietro di diverse versioni: nessuna falla nota attribuita a questa versione.

06 Perimetro, metodo e limiti

Perimetro

- `aziendatest.example`
- `www.aziendatest.example`
- `staging.aziendatest.example`

Metodo

Analisi esterna «black box», dal 10/11/2026 al 12/11/2026: solo ciò che è visibile da internet, senza credenziali, con verifiche non distruttive. Nessun exploit, nessun test di carico, nessun file esposto aperto o scaricato.

Limiti

- Non garantisce che il sito sia sicuro, né che non ci saranno attacchi in futuro.
- Fotografa il sito nelle date indicate: un aggiornamento o un plugin nuovo cambiano il quadro.
- Copre solo il perimetro concordato: rete interna, computer dell'ufficio ed email del personale restano fuori.
- Non corregge: le correzioni le applichi tu o il tuo fornitore, seguendo il report.

DOMANDE SUL REPORT

Per 14 giorni di calendario puoi scriverci a **reports@nulltrace.systems**. La prima risposta nel merito arriva entro 3 giorni lavorativi.

Questo è un esempio con dati fittizi. Il report che riceverai ha la stessa struttura, ma può essere più o meno ricco a seconda di ciò che emerge sul tuo sito.

ESEMPIO · DATI FITTIZI