majhenlabs

Sigurnosni izvještaj

primjer-tvrtka.hr

Datum: 20.07.2026.

Pregled: 8 nalaza

2 visoko | 3 srednje | 1 nisko | 2 info

Nalazi

Baza ili sličan servis je izravno dostupan s interneta

VISOKO

`3306/tcp — MySQL`

Ovo su servisi koji čuvaju podatke i nisu namijenjeni javnom internetu — sajt im pristupa iznutra, s istog poslužitelja.

Zašto je ovo najozbiljniji nalaz u ovom izvještaju: dio ovih servisa povijesno NEMA lozinku dok je netko izričito ne postavi (Redis, MongoDB, Elasticsearch, Memcached). Tko ih nađe otvorene, često ih može pročitati i obrisati bez ijedne lozinke. Automati koji ih traže prolaze cijelim internetom neprekidno — nije pitanje hoće li naići, nego kad.

Mi smo samo provjerili je li port otvoren. Nismo se pokušali spojiti ni bilo što pročitati.

Popravak:

Zatvorite ih prema internetu. Ispravno je da slušaju samo na 127.0.0.1 (ako su na istom poslužitelju kao sajt) ili da im pristup dopusti vatrozid samo s IP adrese koja ih treba. MySQL: bind-address = 127.0.0.1. PostgreSQL: listen_addresses = 'localhost'. Redis/MongoDB: bind 127.0.0.1 i obavezno lozinka.

Ako je nešto od ovoga NAMJERNO javno jer se spaja s druge lokacije — onda treba vatrozid koji pušta samo tu adresu, i šifrirana veza. To više nije klik u panelu.

Dodatak Contact Form 7 5.7.1 — Contact Form 7 < 5.8.2 — Authenticated (Editor+) Arbitrary File Upload

VISOKO

CVE-2023-6449 · CVSS 8.8

The Contact Form 7 plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in versions up to, and including, 5.8.1. This makes it possible for authenticated attackers, with editor-level access and above, to upload arbitrary files on the affected site's server, which may make remote code execution possible.

Tip slabosti: Unrestricted Upload of File with Dangerous Type.

Popravak:

Nadogradite Contact Form 7 na verziju 5.8.2 ili noviju. U wp-adminu: Dodaci → Instalirani dodaci → pronađite Contact Form 7 → Ažuriraj. Prije nadogradnje napravite sigurnosnu kopiju (backup) baze i datoteka. Nakon nadogradnje otvorite naslovnicu i jednu podstranicu da provjerite da se ništa nije razbilo.

Domena nema DMARC zapis — bilo tko može slati mail u vaše ime

SREDNJE

DMARC govori poslužitelju primatelja što učiniti s mailom koji tvrdi da dolazi s vaše domene, a ne prođe provjeru. Bez njega ta odluka ostaje na primatelju i najčešće znači: propusti.

Praktično: netko upiše vašu adresu kao pošiljatelja i pošalje račun vašem kupcu s vlastitim IBAN-om. Mail izgleda kao vaš jer PIŠE da je vaš. Nije potreban nikakav proboj sajta — dovoljno je da domena nema DMARC.

Ograničenje, da ne bude nesporazuma: DMARC štiti VAŠU domenu od krivotvorenja. Ne zaustavlja mail poslan s tuđe adrese na kojoj samo prikazano ime glasi kao Vaše, i ne štiti od sličnih domena.

Popravak:

Dodajte TXT zapis tamo gdje Vam je DNS (najčešće kod registrara domene):

```
ime: _dmarc.primjer-tvrtka.hr
tip: TXT
vrijednost: v=DMARC1; p=none; rua=mailto:postmaster@primjer-tvrtka.hr
```

NE stavljajte odmah p=reject. Redoslijed je namjeran: krenite s p=none, dva do tri tjedna čitajte rua izvještaje i nađite svakog legitimnog pošiljatelja, pa tek onda pređite na p=quarantine, i naposljetku p=reject. Tko preskoči te korake i odmah stavi p=reject, sam sebi ugasi izlazne račune.

Dodatak Elementor 3.18.0 — Elementor <= 3.18.1 — Authenticated (Contributor+) Stored Cross-Site Scripting

SREDNJE

CVE-2023-47505 · CVSS 6.4

The Elementor Website Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via uploaded SVG files in versions up to, and including, 3.18.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

Tip slabosti: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting').

Popravak:

Nadogradite Elementor na verziju 3.18.2 ili noviju. U wp-adminu: Dodaci → Instalirani dodaci → pronađite Elementor → Ažuriraj. Prije nadogradnje napravite sigurnosnu kopiju (backup) baze i datoteka.

Servisi za daljinski pristup su otvoreni prema internetu

SREDNJE

```
21/tcp — FTP
```

FTP i Telnet prenose korisničko ime i lozinku u čitljivom obliku — tko je bilo gdje na putu, može ih pročitati. RDP, VNC i SMB su omiljene mete automatiziranog pogađanja lozinki i povremeno imaju ranjivosti koje ne traže ni lozinku.

Ovo nije nalaz da je netko ušao. Nalaz je da vrata postoje i da ih bilo tko može pokušati otvoriti, koliko god puta hoće.

Popravak:

FTP zamijenite SFTP-om (ide preko SSH-a, port 22) — kod većine hostinga je to već dostupno i samo treba prestati koristiti stari FTP. Telnet nema opravdanja ni u jednom scenariju; ugasite ga. RDP i VNC ne bi smjeli biti izravno na internetu. Ispravno je pustiti ih samo kroz VPN, ili im vatrozidom dopustiti samo IP adrese s kojih se stvarno spajate.

Nema zaštite od ugradnje stranice u tuđi okvir (clickjacking)

NISKO

Bez ovoga bilo tko može učitati vašu stranicu u nevidljivi okvir na svojoj, prekriti je svojim sadržajem i navesti posjetitelja da klikne nešto što misli da je njegovo, a zapravo je vaše.

Iskoristivost je u praksi ograničena i traži da korisnik dođe na napadačevu stranicu. Za sajt bez prijave i bez radnji jednim klikom ovo je uglavnom teorija — navodimo ga jer je popravak trivijalan.

Popravak:

Dodajte jedno od ovoga na sve odgovore:

```
X-Frame-Options: SAMEORIGIN
```

ili, ako već koristite CSP: Content-Security-Policy: frame-ancestors 'self'. Ako sajt negdje NAMJERNO ugrađujete u tuđu stranicu (npr. widget kod partnera), umjesto 'self' navedite točno tu domenu.

Otvoreno je 5 od 23 provjerenih portova

INFO

```
21/tcp — FTP
80/tcp — HTTP
443/tcp — HTTPS
587/tcp — SMTP (submission)
3306/tcp — MySQL
```

Provjerili smo dvadesetak poznatih portova, ne sve. Otvoren port sam po sebi nije problem — SSH, SMTP i slični tu i pripadaju.

Važno ograničenje: provjerili smo IP na koji domena pokazuje. Ako je sajt iza CDN-a ili proxyja, to je njihov poslužitelj, a ne vaš — u tom slučaju ovaj popis govori o njima.

Popravak:

Nema se što popraviti dok se popis ne pročita. Za svaki port se pitajte treba li biti dostupan cijelom internetu ili samo Vama.

Nema Content-Security-Policy zaglavlja

INFO

CSP je popis izvora s kojih stranica smije učitavati skripte i stilove. Kad postoji i kad je dobro napisan, otežava iskorištavanje XSS-a.

NIJE ranjivost. Nedostatak CSP-a ne znači da sajt ima rupu — znači da nema jedan sloj obrane u dubinu. Golema većina sajtova ga nema, i zato ga vodimo kao informaciju, a ne kao problem. Ako Vam netko za ovo da ocjenu 'F', prodaje Vam strah.

Popravak:

Za postojeći sajt CSP se ne piše napamet: prestrog popis razbije vlastite skripte, analitiku i ugrađene sadržaje, a prelabav ne radi ništa. Postupak je krenuti s Content-Security-Policy-Report-Only, skupljati prijave i tek onda uključiti pravi. Ovo je posao za čovjeka i nije hitan.

Robert Majhen, MajhenLabs