

example.com

FECHA DEL ESCANEOD 21/09/2026, 08:00	ALCANCE Pasivo y activo (con comprobación de puertos) + OpenVAS	HOSTS COMPROBADOS 8	FUENTES crt.sh, certspotter
---	--	------------------------	--------------------------------

PUNTUACIÓN DE EXPOSICIÓN

36 / 100



Prioridad media de todos los hallazgos, de 0 a 100.
Cuanto más baja, mejor.

HALLAZGOS: 10

0 CRÍTICA	3 ALTA	3 MEDIA	4 BAJA
--------------	-----------	------------	-----------

Lo más importante en resumen

Aborde primero estos hallazgos. Combinan una gravedad alta con la importancia del sistema afectado.

PRIOR.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
61	ALTA	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ALTA	vpn.example.com RDP accesible desde internet (puerto 3389) → Cierre el puerto en el cortafuegos o restrínjalo a direcciones IP conocidas.
56	ALTA	shop.example.com Interfaz de administración accesible públicamente (phpMyAdmin) → Hágala accesible solo mediante VPN o una lista de IP permitidas.
34	MEDIA	dev.example.com Sistema de desarrollo o de pruebas accesible públicamente → Protéjalo con inicio de sesión, VPN o lista de IP permitidas y apague los sistemas que ya no se necesiten.
34	MEDIA	mail.example.com El certificado TLS caduca en 9 días → Renueve el certificado y compruebe que la renovación automática funciona.

Todos los hallazgos por host

example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
24	BAJA	La política DMARC es p=none, el correo falsificado no se rechaza → Tras analizar los informes, eleve la política a p=quarantine o p=reject.

www.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
24	BAJA	Versión de software visible en la cabecera Server (Apache/2.4.49) → Desactive la indicación de versión en el servidor web (p. ej., server_tokens off, ServerTokens Prod).
20	BAJA	Falta la cabecera Content-Security-Policy → Defina una Content-Security-Policy que solo permita las fuentes necesarias.

shop.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
56	ALTA	Interfaz de administración accesible públicamente (phpMyAdmin) → Hágala accesible solo mediante VPN o una lista de IP permitidas.
32	MEDIA	Falta la cabecera Strict-Transport-Security → Establezca Strict-Transport-Security: max-age=31536000; includeSubDomains.

mail.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
34	MEDIA	El certificado TLS caduca en 9 días → Renueve el certificado y compruebe que la renovación automática funciona.

vpn.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
61	ALTA	OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	ALTA	RDP accesible desde internet (puerto 3389) → Cierre el puerto en el cortafuegos o restrínjalo a direcciones IP conocidas.

dev.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
34	MEDIA	Sistema de desarrollo o de pruebas accesible públicamente → Protéjalo con inicio de sesión, VPN o lista de IP permitidas y apague los sistemas que ya no se necesiten.

portal.example.com

PRIO.	GRAVEDAD	HALLAZGO Y RECOMENDACIÓN
17	BAJA	Falta la cabecera X-Content-Type-Options → Establezca X-Content-Type-Options: nosniff.

Sin hallazgos

cdn.example.com

Método y límites

Los subdominios proceden de los registros públicos de certificados (Certificate Transparency). Solo se comprobaron los hosts que se resuelven por DNS.

En cada host se comprobaron el certificado TLS, la redirección de HTTP a HTTPS, las cabeceras de seguridad de la página de inicio y las interfaces de administración reconocibles; en el dominio principal, además, SPF y DMARC.

Un escaneo pasivo no comprueba puertos abiertos ni ataca aplicaciones. Muestra lo que es visible desde fuera sin credenciales.

Este informe es una instantánea del momento indicado. La prioridad es una valoración y no sustituye a una prueba de penetración.

Además, se realizó con OpenVAS (Greenbone) un escaneo activo de vulnerabilidades de las direcciones públicas, sobre la base de la titularidad demostrada del dominio. Solo se incluyeron hallazgos con una calidad de detección de al menos el 70 por ciento.

Próximos pasos

Con gusto revisamos el informe con usted y le mostramos cómo veyrisk supervisa su superficie de ataque de forma continua, en lugar de mirar una sola vez.

CONTACTO

neonotu GmbH
Edelsbergstraße 8, 80686 München
+49 89 2000 7975 0 · contact@veyrisk.com