

REPORT · EXTERNAL ATTACK SURFACE

example.com

SCAN TIME 21/09/2026, 08:00	SCOPE Passive and active (with port checks) + OpenVAS	HOSTS CHECKED 8	SOURCES crt.sh, certspotter
--------------------------------	--	--------------------	--------------------------------

EXPOSURE SCORE

36 / 100



Average priority of all findings, 0 to 100. Lower is better.

FINDINGS: 10

0	3	3	4
CRITICAL	HIGH	MEDIUM	LOW

Key points

Address these findings first. They combine high severity with the importance of the affected system.

PRIO	SEVERITY	FINDING AND RECOMMENDATION
61	HIGH	vpn.example.com OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	HIGH	vpn.example.com RDP reachable from the internet (port 3389) → Close the port in the firewall or restrict it to known IP addresses.
56	HIGH	shop.example.com Admin interface publicly reachable (phpMyAdmin) → Make it reachable only via VPN or an IP allow list.
34	MEDIUM	dev.example.com Development or test system publicly reachable → Put it behind a login, VPN or IP allow list, and switch off systems no longer needed.
34	MEDIUM	mail.example.com TLS certificate expires in 9 days → Renew the certificate and check that automatic renewal works.

All findings by host

example.com

PRIIO	SEVERITY	FINDING AND RECOMMENDATION
24	LOW	DMARC policy is p=none, spoofed mail is not rejected → After reviewing the reports, raise the policy to p=quarantine or p=reject.

www.example.com

PRIIO	SEVERITY	FINDING AND RECOMMENDATION
24	LOW	Software version disclosed in Server header (Apache/2.4.49) → Turn off version output in the web server (e.g. server_tokens off, ServerTokens Prod).
20	LOW	Missing Content-Security-Policy header → Define a Content-Security-Policy that only allows the sources you need.

shop.example.com

PRIIO	SEVERITY	FINDING AND RECOMMENDATION
56	HIGH	Admin interface publicly reachable (phpMyAdmin) → Make it reachable only via VPN or an IP allow list.
32	MEDIUM	Missing Strict-Transport-Security header → Set Strict-Transport-Security: max-age=31536000; includeSubDomains.

mail.example.com

PRIIO	SEVERITY	FINDING AND RECOMMENDATION
34	MEDIUM	TLS certificate expires in 9 days → Renew the certificate and check that automatic renewal works.

vpn.example.com

PRIIO	SEVERITY	FINDING AND RECOMMENDATION
61	HIGH	OpenSSH 'regreSSHion' Remote Code Execution Vulnerability (22/tcp) → Update OpenSSH to version 9.8p1 or later.
56	HIGH	RDP reachable from the internet (port 3389) → Close the port in the firewall or restrict it to known IP addresses.

dev.example.com

PRIO	SEVERITY	FINDING AND RECOMMENDATION
34	MEDIUM	Development or test system publicly reachable → Put it behind a login, VPN or IP allow list, and switch off systems no longer needed.

portal.example.com

PRIO	SEVERITY	FINDING AND RECOMMENDATION
17	LOW	Missing X-Content-Type-Options header → Set X-Content-Type-Options: nosniff.

No findings

cdn.example.com

Method and limits

Subdomains come from public certificate transparency logs. Only hosts that resolve in DNS were checked.

For each host we checked the TLS certificate, the HTTP to HTTPS redirect, the security headers of the start page and recognisable admin interfaces, plus SPF and DMARC for the main domain.

A passive scan does not check open ports and does not attack applications. It shows what is visible from outside without credentials.

This report is a snapshot at the stated time. The priority is an assessment and does not replace a penetration test.

In addition, an active vulnerability scan of the public addresses was run with OpenVAS (Greenbone), based on verified ownership of the domain. Only findings with a quality of detection of at least 70 percent were included.

Next steps

We are happy to walk you through this report and show how veyrisk monitors your attack surface continuously instead of looking once.

CONTACT

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