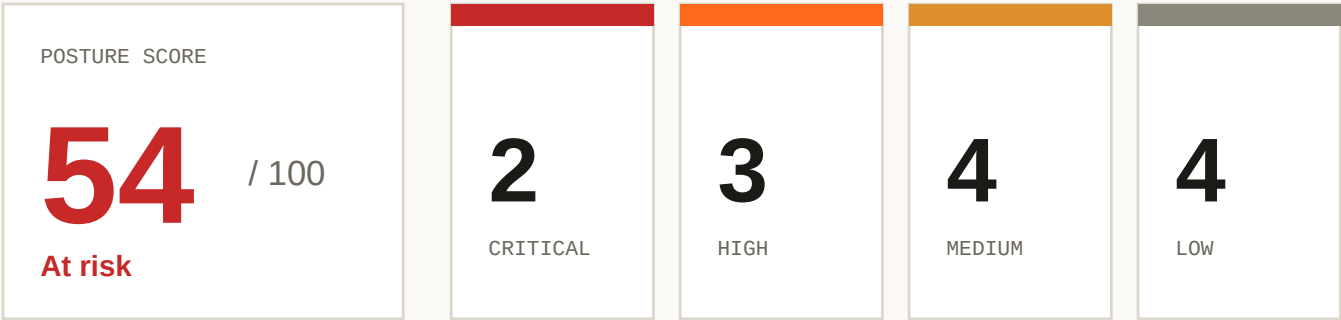


# Daily External Audit

External security posture of an internet-facing estate, as an attacker sees it.

|                |                               |               |                |
|----------------|-------------------------------|---------------|----------------|
| Organisation   | Honeypot-Venture GmbH         | Hosts seen    | 142            |
| Primary domain | honeypot-venture.io           | Subdomains    | 38             |
| Report date    | 2026-10-22                    | Scope         | 5 root domains |
| Audit window   | 02:00 - 06:00 CET (automated) | Data location | Frankfurt, EU  |



This is a demonstration report for a fictional company. It mirrors the structure and the kind of findings a real Athorion daily audit produces, including email authentication, end of life software and exposed services.

The estate exposes two critical issues that allow remote code execution and a set of email and transport weaknesses that make the domain straightforward to impersonate. Two findings are new since yesterday, one earlier issue was resolved. Priority this morning is the GitLab and phpMyAdmin hosts, then the email authentication gap.

Findings by severity



Top risks

|          |                                                                 |                           |
|----------|-----------------------------------------------------------------|---------------------------|
| CRITICAL | GitLab 14.0.1 unauthenticated RCE (CVE-2021-22205, on CISA KEV) | git.honeypot-venture.io   |
| CRITICAL | PHP 5.6 end of life behind a public phpMyAdmin                  | admin.honeypot-venture.io |
| HIGH     | Domain is spoofable: DMARC p=none and no DKIM signing           | honeypot-venture.io       |
| HIGH     | Exposed .git directory leaks source and internal remotes        | www.honeypot-venture.io   |
| HIGH     | Legacy TLS 1.0 / 1.1 and 3DES still accepted                    | shop.honeypot-venture.io  |

Changes since yesterday

- Resolved: 1 (public Redis on cache host, now firewalled)
- New: 2 (GitLab RCE, expired staging certificate)

**CRITICAL** CVSS 10.0 / KEV

git.honeypot-venture.io:443

**GitLab CE 14.0.1 vulnerable to unauthenticated remote code execution (CVE-2021-22205)**

Evidence: Version banner GitLab 14.0.1; the ExifTool image path at /uploads is reachable without authentication. On the CISA Known Exploited Vulnerabilities catalogue.

**Fix:** Upgrade to 14.0.12 / 14.1.7 / 14.2.6 or later today. Treat the host as potentially compromised: rotate runner and CI tokens and review recent jobs.

**CRITICAL** CVSS 9.8

admin.honeypot-venture.io:443

**End of life PHP 5.6.40 exposed behind a public phpMyAdmin**

Evidence: Server header reports PHP/5.6.40 (unsupported since 2018); phpMyAdmin 4.7.0 login page is reachable from the internet and is affected by several known issues.

**Fix:** Move to a supported PHP branch (8.2+). Remove phpMyAdmin from the public internet or bind it to the VPN, and rotate database credentials.

**HIGH** Email

honeypot-venture.io

**The domain can be spoofed: DMARC is monitoring only and mail is not DKIM signed**

Evidence: \_dmarc TXT is v=DMARC1; p=none. No DKIM selector answered (default, google, s1, s2 all NXDOMAIN). SPF is v=spf1 include:\_spf.google.com ~all (softfail).

**Fix:** Publish a DKIM key and sign outbound mail. After a clean reporting window, move DMARC to p=quarantine and then p=reject, and tighten SPF to -all.

**HIGH** Disclosure

www.honeypot-venture.io

**Exposed .git directory discloses source code and internal remotes**

Evidence: /.git/HEAD and /.git/config are fetchable; the config reveals an internal GitLab remote and a deploy user name.

**Fix:** Block /.git at the web server and remove it from the document root. Rotate any credentials present in the repository history.

**HIGH** TLS

shop.honeypot-venture.io:443

**Legacy TLS 1.0 and 1.1 and a weak 3DES cipher are still accepted**

Evidence: The host negotiates TLS 1.0 and 1.1 and offers TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA.

**Fix:** Disable TLS 1.0 and 1.1 and 3DES. Require TLS 1.2 or higher with modern cipher suites.

MEDIUM

End of life

api.honeypot-venture.io

**PHP 7.4.3 is end of life on the API host**

Evidence: X-Powered-By reports PHP/7.4.3; the 7.4 branch has received no security fixes since November 2022.

Fix: Upgrade to PHP 8.2 or later and remove the X-Powered-By header.

MEDIUM

Headers

www.honeypot-venture.io

**Security response headers are missing**

Evidence: No Content-Security-Policy, no X-Frame-Options and no X-Content-Type-Options are set.

Fix: Add a Content-Security-Policy, X-Frame-Options SAMEORIGIN, X-Content-Type-Options nosniff and HSTS.

MEDIUM

Exposure

vpn.honeypot-venture.io:22

**SSH is exposed to the internet with password authentication**

Evidence: OpenSSH 8.2p1 offers keyboard and password authentication to any source address.

Fix: Enforce public key authentication only, restrict by source network and add fail2ban.

LOW

Hygiene

various

**Verbose banners, directory listing, insecure cookies and a softfail SPF**

Evidence: nginx/1.18.0 and OpenSSH 8.2p1 disclose exact versions; /uploads has autoindex on; the shop session cookie lacks Secure and HttpOnly; a staging certificate expired 11 days ago.

Fix: Suppress version tokens, disable autoindex, set Secure, HttpOnly and SameSite on cookies, and renew or decommission the staging host.

Email authentication

|         |                                         |      |
|---------|-----------------------------------------|------|
| SPF     | v=spf1 include:_spf.google.com ~all     | WEAK |
| DKIM    | no selector published, mail is unsigned | FAIL |
| DMARC   | v=DMARC1; p=none (monitoring only)      | WEAK |
| MTA-STX | not found                               | INFO |