



SECURITY REPORT · MULTI-ASSET SUMMARY

# MONTHLY SECURITY REPORT — MARCH 2026

Allen Digital Studio · Sample report — anonymised data

03 Apr 2026 - 03 May 2026

ASSETS

5

SCANS RUN

324

ISSUES FOUND

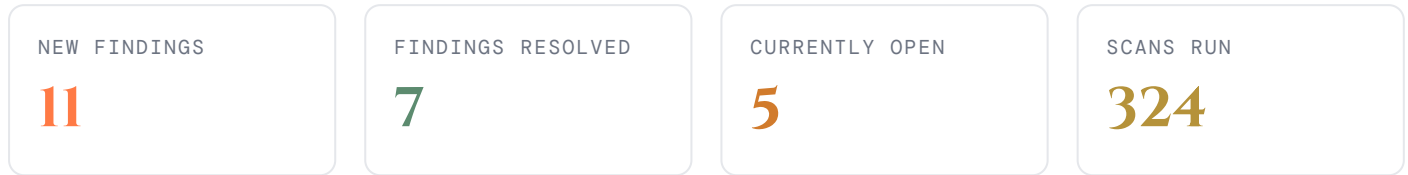
11

ISSUES FIXED

7

# WHAT WE DID FOR YOU THIS PERIOD

Across **5 assets** we ran **324 scans** looking for vulnerabilities, malware, configuration drift, and other security issues. In that time we surfaced **11 new findings** and resolved **7**. As of right now, **5** issues are still open and being tracked.



The pages that follow break down each server and website individually — what was found, what's been fixed, and what's still being tracked. If anything in this report is unclear or you'd like to discuss a specific finding, get in touch with your Astrari team.

# LINUX SERVER FINDINGS

SERVER

## PROD-WEB-01

prod-web-01.allendigital.example

88

SCORE / 100

124 scans run 4 findings opened 3 resolved 1 still open

### NEW THIS PERIOD

HIGH	OpenSSL 3.0.13 — CVE-2024-0727 (DoS via PKCS12)	SRV_PACKAGE_CVE	19 Apr 2026
MEDIUM	PermitRootLogin yes detected in sshd_config	SRV_SSH	14 Apr 2026
MEDIUM	13 OS package updates available (4 with security flags)	SRV_PACKAGE_UPDATE	25 Apr 2026
LOW	Port 8080 reachable from public internet — recommended internal-only	SRV_FIREWALL	24 Apr 2026

### RESOLVED THIS PERIOD

HIGH	OpenSSL 3.0.13 — CVE-2024-0727 (DoS via PKCS12)	SRV_PACKAGE_CVE	19 Apr 2026
MEDIUM	PermitRootLogin yes detected in sshd_config	SRV_SSH	14 Apr 2026
MEDIUM	13 OS package updates available (4 with security flags)	SRV_PACKAGE_UPDATE	25 Apr 2026

### CURRENTLY OPEN

LOW	Port 8080 reachable from public internet — recommended internal-only	SRV_FIREWALL	24 Apr 2026
-----	--	--------------	-------------

SERVER

## STAGING-01

staging-01.allendigital.example

76

SCORE / 100

116 scans run 2 findings opened 0 resolved 2 still open

### NEW THIS PERIOD

MEDIUM	21 OS package updates available (6 with security flags)	SRV_PACKAGE_UPDATE	11 Apr 2026
LOW	/etc/cron.d/staging-deploy modified outside change window	SRV_FILE_INTEGRITY	22 Apr 2026

### CURRENTLY OPEN

MEDIUM	21 OS package updates available (6 with security flags)	SRV_PACKAGE_UPDATE	11 Apr 2026
LOW	/etc/cron.d/staging-deploy modified outside change window	SRV_FILE_INTEGRITY	22 Apr 2026

## WEBSITE FINDINGS

## WEBSITE

## ALLENDIGITAL.EXAMPLE

https://allendigital.example

92

SCORE / 100

28 scans run 2 findings opened 3 resolved 0 still open

## NEW THIS PERIOD

<b>CRITICAL</b>	Contact Form 7 5.7.6 — CVE-2023-6449 (unauthenticated file upload)	WP_PLUGIN_CVE	28 Apr 2026
<b>MEDIUM</b>	Content-Security-Policy header missing	WP_HEADERS	22 Apr 2026

## RESOLVED THIS PERIOD

<b>CRITICAL</b>	Contact Form 7 5.7.6 — CVE-2023-6449 (unauthenticated file upload)	WP_PLUGIN_CVE	28 Apr 2026
<b>MEDIUM</b>	Content-Security-Policy header missing	WP_HEADERS	22 Apr 2026
<b>LOW</b>	WordPress user enumeration via ?author=N is exposed	WP_USER_ENUM	16 Apr 2026

## WEBSITE

## SHOP

https://shop.allendigital.example

81

SCORE / 100

28 scans run 3 findings opened 1 resolved 2 still open

## NEW THIS PERIOD

<b>HIGH</b>	WooCommerce 8.4.0 outdated — current 8.6.1 (3 security advisories)	WP_PLUGIN_OUTDATED	24 Apr 2026
<b>MEDIUM</b>	Session cookie missing Secure and SameSite flags	WP_COOKIES	21 Apr 2026
<b>LOW</b>	DMARC policy is p=none — recommend p=quarantine	WP_EMAIL_AUTH	10 Apr 2026

## RESOLVED THIS PERIOD

<b>MEDIUM</b>	Session cookie missing Secure and SameSite flags	WP_COOKIES	21 Apr 2026
---------------	--	------------	-------------

## CURRENTLY OPEN

<b>HIGH</b>	WooCommerce 8.4.0 outdated — current 8.6.1 (3 security advisories)	WP_PLUGIN_OUTDATED	24 Apr 2026
<b>LOW</b>	DMARC policy is p=none — recommend p=quarantine	WP_EMAIL_AUTH	10 Apr 2026

WEBSITE

## BLOG

https://blog.allendigital.example

95

SCORE / 100

28 scans run 0 findings opened 0 resolved 0 still open

All clear for this period — no new findings, nothing outstanding.

# ASTRARI

Precision security. Human expertise.

A service of **Incus Technologies Limited** (Company No. 09253791).

incuswatch.incustech.app · support@incustech.co.uk