



Vulnerability scanning

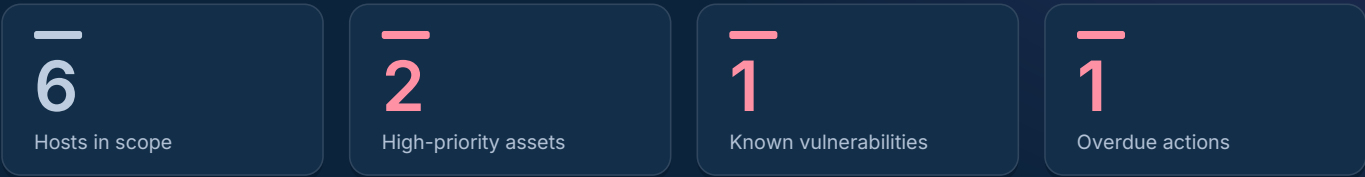
Website security and software vulnerabilities

- 01 Overview
- 02 Assets
- 03 Intelligence
- 04 Actions

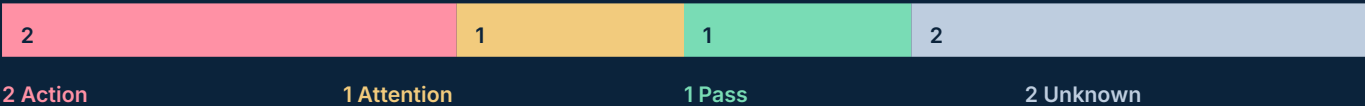
! Action required

Update the portal and enforce email authentication.

The portal uses software with a known exploited vulnerability. DMARC enforcement is also missing.



ASSET STATUS



SECURITY CHECKS

TLS		6/6 pass
Email		0/1 pass
DNS		5/6 pass
Web headers		4/6 pass
Software		4/6 pass

Assessment coverage: 23 of 25 applicable checks returned a result. Grey indicates missing or outdated evidence.

TOP THREE PRIORITIES

- 1

Update the portal software

Application owner / 12 Sep
- 2

Enforce DMARC

Email administrator / 13 Sep
- 3

Add web security headers

Web operations / 18 Sep

CHANGE SINCE 06 SEPTEMBER

Previous	2	1	1	2	2 urgent
Current	2	1	1	2	2 urgent

1 check now passes; one new issue. Both assessments cover the same assets.

6 hosts under northstar.example | Standard scan and linked software inventory

Asset security overview

Security checks for each asset, ordered by priority.

01 Overview

02 Assets

03 Intelligence

04 Actions

! Action

! Attention

+ Pass

? Unknown

ASSET / PLATFORM	TLS	Email	DNS	Web headers	Software
WEB-01 northstar.example	+ Pass	! Action	+ Pass	! Attention	+ Pass
WEB-02 portal.northstar.example	+ Pass	- N/A	+ Pass	+ Pass	! Action
WEB-04 api.northstar.example	+ Pass	- N/A	+ Pass	! Attention	+ Pass
WEB-03 mail.northstar.example	+ Pass	- N/A	? Unknown	+ Pass	+ Pass
WEB-05 admin.northstar.example	+ Pass	- N/A	+ Pass	+ Pass	? Unknown
WEB-06 help.northstar.example	+ Pass	- N/A	+ Pass	+ Pass	+ Pass

N/A checks are excluded from totals. Grey indicates missing or outdated evidence. Software checks do not cover every published vulnerability.

ASSETS AFFECTED BY EACH ISSUE

Add web security headers		2
Update the portal software		1
Enforce DMARC		1
Verify DNSSEC		1

Vulnerabilities and updates

Affected versions, exploitation status and recommended updates.

01 Overview

02 Assets

03 Intelligence

04 Actions

! Affected version confirmed

CVE-2021-44228

Apache Log4j Core

An attacker may be able to run code on the server by sending malicious input that the application logs.


10.0

CVSS 3.1


YES

Known exploitation (KEV)


>99.99%

30-day likelihood


1

Affected hosts

INSTALLED VERSION

2.14.1

ORIGINAL FIX VERSION

2.15.0 (Java 8 and later)

Affected versions: 2.13.0 up to, but excluding, 2.15.0

Evidence: Software inventory identifies log4j-core 2.14.1.

RECOMMENDED UPDATE

Upgrade to the latest supported Log4j release compatible with your application. Test the update before deployment.

The original fix version is historical. Use the latest supported release.

Affected assets: WEB-02

Scope: 1 vulnerability across 1 asset. This report includes selected CVE examples.

Source dates: EPSS 2026-09-12; CISA KEV 2026-09-11; NVD updated 2026-08-11.

EPSS estimates the chance of this vulnerability being exploited in the next 30 days. It does not predict a breach of your organisation. EPSS percentile: 100.00%.

[NVD record](#) | [Apache security advisory](#) | [EPSS explained](#) | [CISA KEV](#)

Remediation plan

Actions, responsible teams, deadlines and verification.

01 Overview	02 Assets	03 Intelligence	04 Actions
5 Open actions	1 Overdue	1 Checks now passing	
01 Update the portal software OVERDUE 12 Sep Install the supported update recommended on page 3 and confirm the version in use. VUL-F01 Application owner 1 asset Open			
02 Enforce DMARC DUE 13 Sep Confirm authorised email senders, then introduce DMARC enforcement in stages. VUL-F02 Email administrator 1 asset Open			
03 Add web security headers DUE 18 Sep Configure HSTS and Content Security Policy headers. Test that the website continues to work correctly. VUL-F03 Web operations 2 assets Open			
04 Verify DNSSEC DUE 14 Sep Check DNSSEC at the authoritative DNS provider and repeat validation. VUL-F04 DNS administrator 1 asset Open			
05 Identify the software version DUE 14 Sep Confirm the product and version used by the administration service before checking for vulnerabilities. VUL-F05 Web operations 1 asset Open			

Before closing an action: record the change and repeat the relevant check. Close the issue once the result confirms that the fix is effective.