VORNIN

ALWAYS WATCHING. ALWAYS WARNING.

CONTINUOUS SCAN REPORT

Vulnerability assessment report

A point-in-time security posture assessment across the configured target set. Findings are classified by severity, mapped to compliance controls, and prioritised for remediation.

REPORT ID VRN-2026-11-27-0900	ISSUED 27 Nov 2026 09:00 UTC
SCOPE 4 Targets observed	HANDLING Confidential · Restricted

PREPARED FOR
Northwind Group

PREPARED BY
Vornin Security

REPORT TYPE
Executive summary

SECTION 01

POSTURE SNAPSHOT

Executive summary

At-risk posture — immediate action required. Snapshot for the period ending 27 November 2026, derived from automated scans across the configured target set.

SECURITY SCORE	OPEN FINDINGS
D · 55	34
of 100, averaged per target	Info excluded
NEEDS ACTION NOW	**SCOPE**
7	4
Critical and High	Targets observed

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	5	12	15	0
Within 1 day.	Within 7 days.	Plan within 30 days.	Within 90 days.	Tracked for trend.

The latest scan of the full scope found 34 open findings: two critical, five high, twelve medium and fifteen low. The two critical findings need action first: the TLS certificate on shop.northwind.example has expired, and northwind/checkout-service ships log4j-core 2.14.1, which is exposed to Log4Shell (CVE-2021-44228), a remote code execution flaw that is actively exploited. The high findings are TLS and certificate weaknesses on the three web hosts and an outdated Django package. Renew the certificate and upgrade log4j-core now, then harden the TLS configuration within the week.

2 Critical and 5 High finding(s) require immediate remediation. Halt non-essential changes until Critical items are resolved.

> Score method: each target starts at 100 and deducts 15 per Critical or High, 5 per Medium and 1 per Low; the report score is the mean of the per-target scores. Grades — A 90+, B 80+, C+ 70+, C 60+, D 50+, F below 50.

RANKED ACTIONS

Priority actions

Deduplicated by finding across hosts, so one misconfiguration on ten hosts reads as one action.

01	**Certificate expired** Renew the SSL certificate immediately	CRITICAL	1 HOST
02	**org.apache.logging.log4j:log4j-core 2.14.1 · CVE-2021-44228** Update org.apache.logging.log4j:log4j-core to a version that resolves CVE-2021-44228.	CRITICAL	1 HOST
03	**Certificate chain issue** Fix certificate chain issues	HIGH	1 HOST
04	**Weak cipher strength** Configure cipher suites with at least 128-bit strength	HIGH	1 HOST
05	**Weak Diffie-Hellman key exchange (Logjam)** Use a DH group of at least 2048 bits (RFC 7919 ffdhe2048+) or disable DHE suites in favour of ECDHE.	HIGH	1 HOST

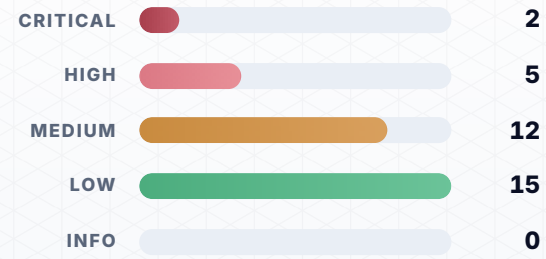
SECTION 02

Distribution & coverage

Severity proportions across the finding set, alongside the targets and scan types this report covers.

Severity distribution

LARGEST CLASS = FULL BAR



Share of all findings — Critical 5% · High 14% · Medium 35% · Low 44% · Info 0%

Report coverage

SCAN TYPES RUN

Targets scanned	4
Total findings	34
Web Application Vulnerabilities	20
SSL/TLS Security	8
Dependency Scanning	5
Nuclei Template Scan	1

SECTION 03

Vulnerabilities by target

4 targets carrying findings, ordered by severity weight.

#	TARGET	CRITICAL	HIGH	MEDIUM	LOW	INFO
01	shop.northwind.example	1	2	4	6	0
02	northwind/checkout-service	1	1	3	0	0
03	api.northwind.example	0	1	3	5	0
04	edge.northwind.example	0	1	2	4	0

SECTION 03 · DETAIL

Target breakdowns

Every finding on each host, grouped by the scan type that produced it.

APPLICATIONS & INFRASTRUCTURE

shop.northwind.example — CRIT · 1 | HIGH · 2 | MED · 4 | LOW · 6

SSL/TLS SECURITY

CRITICAL	Certificate expired
HIGH	Certificate chain issue
HIGH	Weak cipher strength

WEB APPLICATION VULNERABILITIES

MEDIUM	Absence of Anti-CSRF Tokens
MEDIUM	Content Security Policy (CSP) Header Not Set
MEDIUM	Vulnerable JS Library: jquery 1.8.2
MEDIUM	Missing Anti-clickjacking Header
LOW	Strict-Transport-Security Header Not Set
LOW	Cookie without SameSite Attribute
LOW	X-Content-Type-Options Header Missing
LOW	Referrer-Policy Header Not Set
LOW	Server Leaks Version Information via "Server" HTTP Response Header Field
LOW	Permissions Policy Header Not Set

api.northwind.example

HIGH · 1 MED · 3 LOW · 5

NUCLEI TEMPLATE SCAN

LOW	Apache Server Status Disclosure

SSL/TLS SECURITY

HIGH	Weak Diffie-Hellman key exchange (Logjam)

WEB APPLICATION VULNERABILITIES

MEDIUM	Dangerous HTTP Methods Allowed
MEDIUM	Apache server-status exposed
MEDIUM	Content Security Policy (CSP) Header Not Set
LOW	X-Content-Type-Options Header Missing
LOW	Cross-Domain Misconfiguration
LOW	Referrer-Policy Header Not Set
LOW	Permissions-Policy Header Not Set

edge.northwind.example

HIGH · 1 MED · 2 LOW · 4

SSL/TLS SECURITY

HIGH	Deprecated protocol enabled: TLS 1.0
MEDIUM	TLS compression enabled (CRIME)
LOW	TLS_FALLBACK_SCSV not supported
LOW	Root CA certificate included in served chain

WEB APPLICATION VULNERABILITIES

MEDIUM	HTTP Does Not Redirect to HTTPS
LOW	Cross-Origin-Opener-Policy Header Missing or Invalid
LOW	Cross-Origin-Resource-Policy Header Missing or Invalid

CODE & SUPPLY CHAIN

northwind/checkout-service ● CRIT · 1 ● HIGH · 1 ● MED · 3

DEPENDENCY SCANNING

CRITICAL	org.apache.logging.log4j:log4j-core 2.14.1 · CVE-2021-44228
HIGH	Django 3.1.0 · CVE-2022-36359
MEDIUM	urllib3 1.25.7 · CVE-2020-26137
MEDIUM	axios 0.18.0 · CVE-2023-45857
MEDIUM	org.apache.commons:commons-lang3 3.2 · CVE-2025-48924

SECTION 05

Methodology & definitions

How this assessment was produced, how severities are assigned, and how the score is calculated.

5.1 ASSESSMENT METHODOLOGY

Findings in this report were produced by automated, non-destructive scanning of the in-scope targets. No exploitation was attempted and no denial-of-service techniques were used — this is a vulnerability assessment, not a penetration test. Each finding is fingerprinted so that re-scans track the same issue over time; findings that are remediated stop appearing and are automatically marked resolved when a subsequent scan of the same type no longer detects them.

Coverage in this report: Dependency Scanning · Nuclei Template Scan · SSL/TLS Security · Web Application Vulnerabilities.

5.2 SEVERITY DEFINITIONS

SEVERITY	DEFINITION	RECOMMENDED RESPONSE
CRITICAL	Directly exploitable with severe impact: remote code execution, exposed credentials or data, or full system compromise.	Within 1 day (SLA policy)
HIGH	Exploitable weakness with significant impact, or a critical control that is absent or bypassable.	Within 7 days (SLA policy)
MEDIUM	Weakness that increases attack surface or requires specific conditions to exploit.	Within 30 days (SLA policy)
LOW	Minor deviation from hardening best practice with limited direct impact.	Within 90 days (SLA policy)
INFO	Observation with no direct security impact — inventory, version, or configuration context.	No action required; tracked for trend

5.3 SECURITY SCORE

Each target starts at 100 and deducts 15 points per Critical or High finding, 5 per Medium, and 1 per Low (floored at 0); the report score is the average of the per-target scores, so a report covering many targets is not dragged to zero by one noisy host. Info findings never affect the score. Grades: A 90+, B 80+, C+ 70+, C 60+, D 50+, F below 50. The score is a communication device for tracking direction between reporting periods; it is not a substitute for reading the Critical and High findings.

5.4 DISCLAIMER

This report reflects the security posture of the in-scope targets at the time of scanning only. Automated assessment cannot detect every class of vulnerability, and the absence of a finding is not a guarantee that none exists. Severity classifications are advisory and should be validated against the business context of each affected system.

> Questions about this report should be directed to Vornin.