



NIS2 posture report

Acme NIS2 s.r.o. · NIS2-20261014-A1B2C3D4 · 2026-10-14 09:12 UTC

SAMPLE

01 · EXECUTIVE SUMMARY

D

50/100

Material gaps. Two internet-facing assets are exploitable today.

Posture improving. F → D over 90 days.

MOST URGENT: F-01 CVE-2024-3094 · Overdue 6d

312 open

1 KEV

1 overdue

1 CRITICAL

2 HIGH

1 MEDIUM

1,284 assets monitored · +18 new in the last 30 days

02 · EFFECTIVENESS OVER TIME

Change and aging of the exposure register over the last 30 days, plus the raw posture trend across recent assessments. This is a repeatable, independent outside-in measurement usable as one input to the effectiveness assessment NIS2 Art. 21(2)(f) / CIR (EU) 2024/2690 §7 requires; it does not by itself evidence that such a process is operated across the entity’s full control set.

OPEN NOW	NEW (30D)	RESOLVED (30D)
312	18	29
RESOLVED (TOTAL)	OPEN > 30 DAYS	OPEN > 90 DAYS
184	97	12
MEDIAN OPEN AGE (DAYS)	OLDEST OPEN (DAYS)	MEDIAN TIME-TO-REMEDiate (DAYS)
23	199	11

Posture trend

Raw attack-surface score per completed assessment (before triage), newest first.



DATE	DOMAIN	SCORE	GRADE	OPEN	KEV
------	--------	-------	-------	------	-----

2026-10-14	acme.sk	50	D	312	1
2026-09-14	acme.sk	46	F	341	2
2026-08-15	acme.sk	43	F	360	2
2026-07-16	acme.sk	41	F	372	3

03 · SCOPE, METHODOLOGY & RISK RATINGS

SCRY

Scope

This assessment covers the organization's externally reachable attack surface: internet-facing hosts, services, certificates and technologies discovered for the entity, and the vulnerabilities observable on them. It excludes authenticated, internal and physical testing.

Data sources

Findings are gathered by scry's continuous external attack-surface monitoring and enriched with exploitation intelligence (CISA KEV, EPSS, SSVC) and NIS2/CIR mappings from grimoire, temnir's public threat-knowledge graph. Every exposure links back to grimoire for provenance.

Applicable legal framework

EU FRAMEWORK	Directive (EU) 2022/2555 (NIS2) · CIR (EU) 2024/2690
NATIONAL LAW	zákon č. 366/2024 Z. z.(amends the Slovak Cybersecurity Act No. 69/2018, transposing NIS2) · in force since 2025-01-01
COMPETENT AUTHORITY	Národný bezpečnostný úrad(NBÚ)
ENTITY CLASSIFICATION	The Act calls an in-scope organization a «prevádzkovateľ základnej služby» (operator of an essential service). It sets stricter obligations for an operator of a «kritická základná služba» (critical essential service) than for other operators of essential services; unlike some member states, Slovakia kept the operator-of-an-essential-service scheme rather than the directive's essential/important-entity wording. Which category applies is determined by the sector and the size/turnover thresholds in the Act and by NBÚ registration.
TECHNICAL MEASURES	Technical security measures are set by the NBÚ decree vyhláška č. 227/2025 Z. z. (incident reporting by vyhláška č. 226/2025 Z. z.); for digital-service providers, CIR (EU) 2024/2690 applies directly.

An operator of an essential service must undergo a cybersecurity audit at least every two years and after any significant change, performed by a certified cybersecurity auditor («certifikovaný audítor kybernetickej bezpečnosti»); an operator that does not run a critical essential service may in defined cases use a self-assessment («samohodnotenie») instead. This report provides reproducible technical evidence toward the external-attack-surface scope of that audit; it is not the audit, nor a penetration test.

This report describes the applicable framework; it does not determine your essential-service status or category (which depend on your sector and size), and it does not certify NIS2 compliance.

Criteria coverage

EVIDENCED BY THIS REPORT

Vulnerability handling & disclosure

CIR (EU) 2024/2690 · Annex §6.10

Security patch management (EOL / outdated software)

CIR (EU) 2024/2690 · Annex §6.6

Secure configuration & network exposure

CIR (EU) 2024/2690 · Annex §6.3, §6.7

Cryptography (TLS / certificate posture)

CIR (EU) 2024/2690 · Annex §9

Asset management (external inventory)

CIR (EU) 2024/2690 · Annex §12.4

Effectiveness monitoring of measures

CIR (EU) 2024/2690 · Annex §7

NOT COVERED — ASSESSED BY OTHER MEANS

Risk analysis & security policies · Art. 21(2)(a)

Incident handling · (b)

Business continuity & crisis management · (c)

Supply-chain security · (d)

Cyber hygiene & training · (g)

Access control, HR & internal asset security · (i), (j)

This report is technical evidence toward the measures on the left. It does not assess or attest the measures on the right, which require organizational, process and internal-system review beyond an external attack-surface assessment. The CIR (EU) 2024/2690 technical measures are directly binding for the entity types within its scope (DNS, cloud, data-centre, CDN, managed-service and trust-service providers, and similar); for other essential and important entities they are the authoritative reference for the Article 21(2) measures, applied through national law.

Severity ratings

CRITICAL Trivially exploitable with severe impact; treat as an active incident.

HIGH Readily exploitable or high-impact; remediate within days.

MEDIUM Exploitable under conditions or moderate impact; schedule remediation.

LOW Limited exploitability or impact; remediate opportunistically.

Posture score

The A–F grade starts at 100 and deducts for each unhandled exposure by its sharpest signal — known-exploited (KEV) weighs heaviest, then severity, then EPSS. Resolved and accepted exposures are excluded, so triage improves the grade.

Limitations

This is a point-in-time snapshot of externally observable data. Absence of a finding is not proof of security; vulnerabilities are inferred from observed products and versions, not confirmed by exploitation. It reflects the exposure state on the assessment date rather than the operating effectiveness of controls over a period, and it is not a penetration test. Scope: this report evidences the externally observable, technical subset of the NIS2 risk-management measures (CIR (EU) 2024/2690 Annex) — vulnerability handling (§6.10), secure configuration and network exposure (§6.3, §6.7), security patch management (§6.6), effectiveness monitoring (§7), cryptography (§9) and asset management (§12.4). It is a continuous-monitoring attestation of the attack surface, not a full NIS2 conformity assessment.

External attribution can occasionally be wrong (shared hosting, stale DNS records, reassigned addresses). If any asset or finding in this report is misattributed to your organization, report it to your assessment provider so it is corrected and reflected in the next assessment.

Evidence handling & integrity

Every exposure links back to grimoire for provenance and carries the time it was last observed and the reference of the scan that recorded it. Each report carries a SHA-256 content-integrity digest computed over its finding set and entity identity: the same underlying assessment data reproduces the same digest, so undetected alteration of this document is evident. The digest is an integrity check, not a cryptographic signature. Underlying scan findings are retained per temnir's published data-retention policy (365 days); this report is a point-in-time artifact, regenerated on demand rather than separately stored.

04 · NIS2 DUTIES AT RISK

Vulnerability handling and disclosure ↗ CIR (EU) 2024/2690 · Annex §6.10	3 breaching
Network security ↗ CIR (EU) 2024/2690 · Annex §6.7	1 breaching
Security patch management ↗ CIR (EU) 2024/2690 · Annex §6.6	1 breaching
Configuration management ↗ CIR (EU) 2024/2690 · Annex §6.3	1 breaching

05 · FINDINGS

F-01

CRITICAL

KEV

CVE-2024-3094

OPEN

AFFECTED ASSET

build-01

CVSS

10.0

EPSS

94.0%

SSVC

Act

OBSERVED

2026-10-14 09:12 UTC

FIRST OBSERVED

2026-03-29 · 199 days

DESCRIPTION:

Malicious code introduced into upstream xz/liblzma releases 5.6.0 and 5.6.1 (the xz-utils backdoor) grants remote, unauthenticated code execution via a compromised sshd on an internet-facing build host.

IMPACT:

This vulnerability is in CISA's Known Exploited Vulnerabilities catalog — it is being actively exploited in the wild, so the exposure is a live, high-likelihood risk.

REMEDIATION:

Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.

REFERENCES:

CVE-2024-3094 ↗ CWE-506 ↗ CIR (EU) 2024/2690 · Annex §6.10 ↗
Evidence ref: 8f2a9c3d

F-02

HIGH

SSA-818183

OPEN

AFFECTED ASSET

plc-floor2 · OT

CVSS

7.5

SSVC

Attend

OBSERVED

2026-10-14 09:12 UTC

FIRST OBSERVED

2026-10-02 · 12 days

DESCRIPTION: Siemens SIMATIC S7-1500 CPU running firmware 2.9 is reachable from the IT VLAN. The affected firmware is covered by Siemens advisory SSA-818183; the controller should not be routable from general-purpose networks.

IMPACT: A known vulnerability is exposed on an internet-facing service; an attacker who reaches it could exploit it to the extent the vulnerability allows.

REMEDIATION: Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.

REFERENCES: [SSA-818183](#) ↗ [CWE-306](#) ↗ [CIR \(EU\) 2024/2690 · Annex §6.10](#) ↗

Evidence ref: 1b77e4a0

F-03

HIGH

Internet-exposed remote access

OPEN

AFFECTED ASSET

vpn-gw.acme.sk:3389

OBSERVED

2026-10-14 09:12 UTC

FIRST OBSERVED

2026-09-20 · 24 days

DESCRIPTION: Microsoft RDP (TCP/3389) is reachable from the public internet on the VPN gateway, presenting a brute-force and exploitation surface for remote access.

IMPACT: This exposure sits on an internet-facing asset and weakens the security of the affected service; left open, an attacker who reaches it can take advantage of it.

REMEDIATION: Put remote access behind a VPN, firewall the port, and require MFA.

REFERENCES: [CWE-284](#) ↗ [CIR \(EU\) 2024/2690 · Annex §6.7](#) ↗ Evidence ref: c039ab12

F-04

MEDIUM

CVE-2023-0464

OPEN

AFFECTED ASSET

mail-01.acme.sk

CVSS

7.5

EPSS

12.3%

SSVC

Attend

OBSERVED

2026-10-14 09:12 UTC

FIRST OBSERVED

2026-09-11 · 33 days

DESCRIPTION: OpenSSL 1.1.1t on the mail relay is affected by CVE-2023-0464 (excessive resource use when verifying X.509 policy constraints), enabling denial of service against TLS termination.

IMPACT: A known vulnerability is exposed on an internet-facing service; an attacker who reaches it could exploit it to the extent the vulnerability allows.

REMEDIATION: Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.

REFERENCES: [CVE-2023-0464](#) ↗ [CWE-295](#) ↗ [CIR \(EU\) 2024/2690 · Annex §6.10](#) ↗

Evidence ref: 5de1f8c4

F-05

LOW

End-of-life software

OPEN

AFFECTED ASSET

OBSERVED

FIRST OBSERVED

fw-edge-01.acme.sk 2026-10-14 09:12 UTC 2026-05-02 · 165 days

DESCRIPTION: The edge firewall appliance runs a firmware train that reached end-of-life in 2024 and no longer receives security fixes from the vendor.

IMPACT: This exposure sits on an internet-facing asset and weakens the security of the affected service; left open, an attacker who reaches it can take advantage of it.

REMEDIATION: Upgrade to a vendor-supported release; end-of-life software receives no security patches.

REFERENCES: CIR (EU) 2024/2690 · Annex §6.6 ↗ Evidence ref: a7c20b9e

F-06 LOW Exposed admin panel

OPEN

AFFECTED ASSET OBSERVED FIRST OBSERVED
hmi-floor1.acme.sk · OT 2026-10-14 09:12 UTC 2026-08-14 · 61 days

DESCRIPTION: An administrative web panel (HMI) for a floor controller is exposed without network restriction and responds on the public interface, in places still carrying vendor-default credentials.

IMPACT: This exposure sits on an internet-facing asset and weakens the security of the affected service; left open, an attacker who reaches it can take advantage of it.

REMEDIATION: Restrict the admin/actuator endpoint to an allowlist or VPN and require authentication.

REFERENCES: CWE-1392 ↗ CIR (EU) 2024/2690 · Annex §6.3 ↗ Evidence ref: f41d6677

06 · PRIORITIZED REMEDIATION

Actions ordered by priority — known-exploited vulnerabilities first.

Target = the remediation window for each severity, measured from first observation, per this organization's policy. A target for accountability, not a regulatory deadline or a committed SLA.

PRIORITY	TARGET	FINDING	RECOMMENDED ACTION
IMMEDIATE	Overdue 6d	F-01 CVE-2024-3094	Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.
HIGH	Due in 2d	F-02 SSA-818183	Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.
HIGH	Due in 5d	F-03 Internet-exposed remote access	Put remote access behind a VPN, firewall the port, and require MFA.
MEDIUM	Due in 23d	F-04 CVE-2023-0464	Update the affected product to a fixed version per the vendor advisory; where no fix exists, apply the documented mitigation or remove the service from exposure.
LOW	Due in 48d	F-05 End-of-life software	Upgrade to a vendor-supported release; end-of-life software receives no security patches.
LOW	Due in 61d	F-06 Exposed admin panel	Restrict the admin/actuator endpoint to an allowlist or VPN and require authentication.

Generated by temnir · sigil · NIS2 posture report. Evidences the technical subset of CIR (EU) 2024/2690; not a full NIS2 conformity assessment. Figures are as of the generation time above.