

Supply Chain Risk Management



Why?

Moldova adopted the EU-backed Cybersecurity Law

🕒 11.05.2023 👤 Press and information team of the Delegation to MOLDOVA

The newly adopted national cybersecurity law of Moldova was published in the Official Gazette of the Republic of Moldova on May 2nd and will enter into force in Moldova on January 1st, 2025. The national cybersecurity law was drafted with the support of European Union's Moldova cyber security rapid assistance project.

Article 21:

2 (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;

2 (e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

■ Legea 48/2023

Cap. III, Art. 11:

2 (h) măsurile privind asigurarea securității lanțului de aprovizionare, inclusiv aspectele, legate de securitate, referitoare la relațiile furnizorului de servicii cu prestatorii sau cu furnizorii direcți de servicii ai acestuia;



That's all Folks!

■ Breach is simple



CVE-2025-4802 (10.0)

Untrusted LD_LIBRARY_PATH environment variable allows attacker load dynamically shared library

CVE-2025-21298 (9.8)

MS Zero-Click RCE Vulnerability

EUVD-2025-14705 (9.6)

A stack-based buffer overflow vulnerability [CWE-121] in Fortinet

■ Third-Party Data Breach

NotPetya (2017)

Target a Ukrainian accounting software package

Microsoft (2021)

HAFNIUM attacks, compromised the on-premises Microsoft Exchange Servers of 30,000 organizations

38 million records were exposed

SolarWinds (2020)

Comprised a multistage process, scanning downstream customer networks to detect security tools it could avoid or disable, and stealthily connecting to the attacker's command and control servers

Bitsight's analysis quantified the insured losses from the attack at \$90,000,000

Toyota (2022)

Kojima Industries – was hit by a cyber attack

Suspended production at 14 manufacturing plants

MD example

<div>Score</div> <div>935.1</div>				
<div>Accumulated CVSS Score ⓘ</div> <div>The figure to the left is the accumulated score of all vulnerabilities detected for this view.</div> <div>For more information see: First Org CVSS Specification</div>				
Vul ID	IP	Port	CVE	CVSS
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	10	Critical
🔒	📄 xx.xx.xx.xx	⚙️	9.4	Critical
🔒	📄 xx.xx.xx.xx	⚙️	9	Critical

4,163	Hikvision	1,803	HTTP
59	Microsoft	569	RTSP
51	MikroTik	217	UNKNOWN
38	redhat	172	HIKVISION
17	Apache	47	MIKROTIK_BW
17	DahuaSecurity	44	L2TP
14	Linux	42	RDP
10	DrayTek	34	PPTP
10	nginx	23	IKE
9	Huawei	18	DNS
9	microsoft	15	SSH
8	TP-LINK	12	FTP
7	Boa	7	SMTP
6	Filezilla-Project	7	VNC
5	Genivia	6	SNMP
4	CentOS	4	DVR_IP
4	Debian	4	EZVIZ
4	Dropbear SSH Project	4	IMAP
4	Postfix	4	MSSQL
4	Python Software Foundation	3	CWMP

■ Vendor problems example

[] in 2025

CVE-2025-32756: CVE 9.8

CVE-2025-24472: CVE 9.8

CVE-2024-55591: CVE 9.6

CVE-2023-37936: CVE 9.6

[] in 2024

CVE-2024-21762: CVE 9.8

CVE-2024-23113: CVE 9.8

CVE-2024-47575: CVE 9.8

(in 2025

CVE-2025-20124: CVE 9.9

CVE-2025-20125: CVE 9.1

CVE-2025-20156: CVE 9.9

(in 2024

CVE-2024-20440: CVE 9.8

0 in 2025

CVE: None > 9.0

0 in 2025

CVE: None > 9.0

■ Business impact

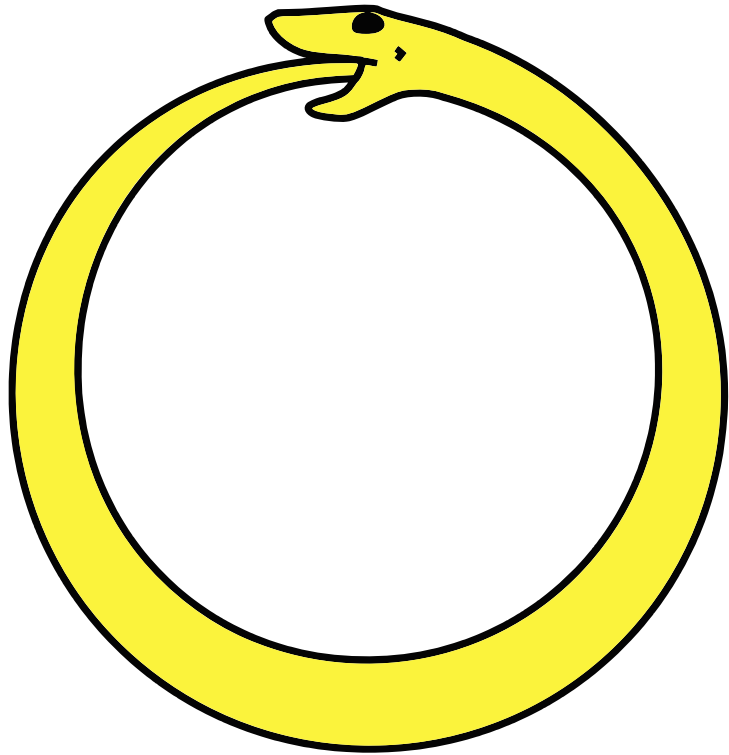
- Operational disruption: Average downtime cost of \$8,851 per minute
- Compliance violations: Potential regulatory fines up to 4% of global revenue
- Customer data exposure: Avg. cost of \$150 per compromised record
- Reputation damage: 60% of SMBs close within 6 months of major breach
- Competitive disadvantage: Recovery time averages 279 days

■ The Costs

Type of Breach	Average Cost*
Average Global Data Breach	\$4.88 Million
Average Finance Sector Data Breach	\$6.08 Million
Average Healthcare Sector Data Breach	\$9.8 Million
Average Industrial Sector Data Breach	\$5.56 Million
Average Small/Medium Business (SMB) Breach	\$120k - \$3.31M

* <https://www.ibm.com/reports/data-breach>

■ Evaluating



- Regulatory Alignment
- Security Certifications
- Vulnerability Management
- Incident History
- Development Practices
- Third-party Assessments
- Financial Stability
- AI System Governance

■ Security Mindset

- Implements quantum-resistant algorithms in TLS VPN solutions
- Published independent validation results:
FIPS, ISO, ICSA Labs, CSfC, NSS, SOC 2, etc.
- Provides detailed cryptographic implementation documentation upon request
- Secure SDLC
- Zero Trust Network Access (ZTNA) architecture in own operations



■ Secure by Design




- Insufficient testing and quality control
- Limited transparency
- Recurring pattern of significant issues
- Incident History
- Independent PSIRT team
- Independent audits
- AI compliance


■ Keys to succeed

- NIST SP 800-161: A Comprehensive Framework
- C-Level Ownership
- C-CSR Program: clear roles and programs
- Prediction costs less
- Not all vendors are equal
- Vendor Transparency
- Use AI/Automation



Thank you!

 MD-2069, Moldova,
Chisinau, str. Calea Iesilor 10

 (+373 22) 509-709
(+373 22) 509-710

 www.daacdigital.com
info@dsi.md