External scan report · 18 November 2026

jusu-imone.lt

The cybersecurity requirements for NIS2 entities include a vulnerability scan at least every six months. This report is the external part of it: what your systems show the internet. It does not cover the internal network, workstations or systems behind a login.

Serious problems	Serious vulnerabilities	Exploited in the wild	Out of support
2	2	1	1

Software we can see from outside

Apache HTTP Server 2.4.41	Server header	**Confirm the package version**	Cycle 2.4
CVE-2021-44790 · 9.8	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser of Apache HTTP Server 2.4.51 and earlier.		
The version was read from the server's banner. Linux distributions (Ubuntu, Debian and others) often apply security fixes without changing the version number, so confirm these against the package version.			
PHP 7.4.3	response header	**Out of support**	Cycle 7.4 · until 2022-11-28
OpenSSH 8.2p1	SSH banner	**Confirm the package version**	
CVE-2023-38408 · 9.8 · KEV	The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system.		
CVE-2023-48795 · 5.9	The SSH transport protocol with certain OpenSSH extensions allows remote attackers to bypass integrity checks (Terrapin).		
The version was read from the server's banner. Linux distributions (Ubuntu, Debian and others) often apply security fixes without changing the version number, so confirm these against the package version.			
WordPress 6.1.1	page source	**Outdated version**	
jQuery 3.4.1	page source	**Outdated version**	
CVE-2020-11022	Potential XSS vulnerability in jQuery		

Findings register

Findings register: fill in the owner and the date it will be fixed – the register fits with your security records.

Severity	Finding and how to fix it	Owner	By
Medium	**4 security headers missing** Browsers get no instructions on how to protect your visitors. 1. Add the missing headers in the server settings.		
Minor	**The server announces its version** The headers show Apache/2.4.41 (Ubuntu), PHP/7.4.3. 1. Hide the version in the server settings.		

This is a technical check of what is publicly visible, not legal advice, a certification or an audit. It reflects the state on the day of the check and does not assess what cannot be seen from outside. Our liability is limited to the price paid.

Minor	**No security.txt** Someone who finds a flaw doesn't know whom to tell. 1. Publish /.well-known/security.txt with a contact.		
Medium	**WordPress is out of date** Version 6.1.1, latest 6.8.3: security fixes missed. 1. Back up, then update. 2. Turn on automatic updates.		
Medium	**2 plugins out of date** For example contact-form-7 5.7.2 → 6.0; elementor 3.12.1 → 3.25.4. 1. Update the plugins. 2. Delete the ones you don't use.		
Minor	**xmlrpc.php is switched on** It makes mass password guessing easy. 1. Turn XML-RPC off if you don't use it.		
Minor	**The admin login is open to everyone** /wp-login.php opens from anywhere. 1. Add two-step login and a rate limit.		
Medium	**Outdated jQuery 3.4.1 with a known flaw** The site runs jQuery 3.4.1. 1. Update the library or the theme that loads it.		
Minor	**SPF only warns** With ~all, forged mail often still gets delivered. 1. Once DMARC is in place, move to -all.		
Serious	**Anyone can send email as you** There is no DMARC record, so forged mail is not refused. 1. Add the TXT record below. 2. After 2 weeks change p=none to p=quarantine.		
Minor	**Mail to you may travel unencrypted** Without MTA-STS, encryption can be stripped on the way. 1. Publish an MTA-STS policy and the _mta-sts record.		
Serious	**The database is reachable from the internet** Port 3306 accepts connections from anywhere. 1. Close the port in the firewall. 2. Change the database password.		
Medium	**A forgotten copy of the site** test.jusu-imone.lt opens without a password. 1. Delete copies you don't need and their DNS records. 2. Put a password on the rest.		
Medium	**The certificate expires in 8 days** If auto-renewal fails, visitors will see “Connection not private”. 1. Turn on auto-renewal in your hosting panel.		
Minor	**No CAA record** Any certificate authority may issue for your domain. 1. Allow only the authority you use.		

This is a technical check of what is publicly visible, not legal advice, a certification or an audit. It reflects the state on the day of the check and does not assess what cannot be seen from outside. Our liability is limited to the price paid.

Minor	**The domain has no DNSSEC** DNS answers cannot be verified, so they are easier to forge. 1. Turn on DNSSEC at your registrar.	

Method and limits

We checked mail records (SPF, DKIM, DMARC), the TLS certificate and protocols, website headers and public files, subdomains from certificate logs, and open services on the server. Software versions were matched against the NVD and OSV vulnerability databases, support terms against endoflife.date, and actively exploited vulnerabilities against the CISA KEV list.

Data sources: NVD (nvd.nist.gov) · OSV (osv.dev) · endoflife.date · CISA Known Exploited Vulnerabilities

This is a technical check of what is publicly visible, not legal advice, a certification or an audit. It reflects the state on the day of the check and does not assess what cannot be seen from outside. Our liability is limited to the price paid.