Išorinio skenavimo ataskaita · 2026 m. lapkričio 18 d.

# jusu-imone.lt

NIS2 subjektams taikomi kibernetinio saugumo reikalavimai numato pažeidžiamumų skenavimą ne rečiau kaip kas šešis mėnesius. Ši ataskaita – išorinė jo dalis: ką jūsų sistemos rodo internetui. Vidinio tinklo, darbo vietų ir prisijungimą reikalaujančių sistemų ji neapima.

| Rimtos problemos | Rimti pažeidžiamumai | Aktyviai išnaudojami | Be palaikymo |
|---|---|---|---|
| 2 | 2 | 1 | 1 |

## Programinė įranga, kurią matome iš išorės

**Apache HTTP Server 2.4.41** — serverio antraštė — **Patikrinkite paketo versiją** — Ciklas 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.

Versija perskaityta iš serverio pranešimo. Linux distribucijos (Ubuntu, Debian ir kt.) saugumo pataisas dažnai įdiegia nekeisdamos versijos numerio, todėl šiuos pažeidžiamumus patikrinkite pagal paketo versiją.

**PHP 7.4.3** — atsakymo antraštė — **Palaikymas baigėsi** — Ciklas 7.4 · iki 2022-11-28

**OpenSSH 8.2p1** — SSH pasisveikinimas — **Patikrinkite paketo versiją**

- **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).

Versija perskaityta iš serverio pranešimo. Linux distribucijos (Ubuntu, Debian ir kt.) saugumo pataisas dažnai įdiegia nekeisdamos versijos numerio, todėl šiuos pažeidžiamumus patikrinkite pagal paketo versiją.

**WordPress 6.1.1** — puslapio kodas — **Pasenusi versija**

**jQuery 3.4.1** — puslapio kodas — **Pasenusi versija**

- **CVE-2020-11022** — Potential XSS vulnerability in jQuery

## Radinių registras

Radinių registras: įrašykite atsakingą asmenį ir datą, iki kada sutvarkysite – registras tinka prie jūsų saugumo dokumentų.

| Svarba | Radinys ir kaip taisyti | Atsakingas | Iki |
|---|---|---|---|
| Vidutinė | **Trūksta 4 saugumo antraščių**<br>Naršyklė negauna nurodymų, kaip apsaugoti lankytojus.<br>1. Pridėkite trūkstamas antraštes serverio nustatymuose. | | |
| Smulki | **Serveris skelbia savo versiją**<br>Antraštėje matyti Apache/2.4.41 (Ubuntu), PHP/7.4.3.<br>1. Paslėpkite versiją serverio nustatymuose. | | |

| | | | |
|---|---|---|---|
| Smulki | **Nėra security.txt**<br>Radęs spragą žmogus nežino, kam apie ją pranešti.<br>1. Paskelbkite /.well-known/security.txt su kontaktu. | | |
| Vidutinė | **WordPress neatnaujinta**<br>Versija 6.1.1, naujausia 6.8.3: praleisti saugumo pataisymai.<br>1. Pasidarykite kopiją ir atnaujinkite.<br>2. Įjunkite automatinius atnaujinimus. | | |
| Vidutinė | **2 įskiepiai neatnaujinti**<br>Pvz., contact-form-7 5.7.2 → 6.0; elementor 3.12.1 → 3.25.4.<br>1. Atnaujinkite įskiepius.<br>2. Ištrinkite nenaudojamus. | | |
| Smulki | **Įjungtas xmlrpc.php**<br>Per jį patogu masiškai spėlioti slaptažodžius.<br>1. Išjunkite XML-RPC, jei jo nenaudojate. | | |
| Smulki | **Administravimo prisijungimas atviras visiems**<br>/wp-login.php atsidaro iš bet kur.<br>1. Įjunkite dviejų žingsnių prisijungimą ir bandymų ribą. | | |
| Vidutinė | **Pasenusi jQuery 3.4.1 su žinoma spraga**<br>Svetainėje veikia jQuery 3.4.1.<br>1. Atnaujinkite biblioteką ar temą, kuri ją įkelia. | | |
| Smulki | **SPF tik įspėja**<br>Su ~all suklastoti laiškai dažnai vis tiek pasiekia gavėją.<br>1. Kai DMARC veikia, pereikite prie -all. | | |
| Rimta | **Bet kas gali siųsti laiškus jūsų vardu**<br>Nėra DMARC įrašo, todėl suklastoti laiškai neatmetami.<br>1. Pridėkite žemiau esantį TXT įrašą.<br>2. Po 2 savaičių pakeiskite p=none į p=quarantine. | | |
| Smulki | **Laiškai jums gali keliauti be šifravimo**<br>Nėra MTA-STS, todėl šifravimo galima išvengti pakeliui.<br>1. Paskelbkite MTA-STS politiką ir _mta-sts įrašą. | | |
| Rimta | **Duomenų bazė pasiekiama iš interneto**<br>Prievadas 3306 priima prisijungimus iš bet kur.<br>1. Uždarykite prievadą ugniasienėje.<br>2. Pakeiskite duomenų bazės slaptažodį. | | |
| Vidutinė | **Pamiršta svetainės kopija**<br>test.jusu-imone.lt atidaroma be slaptažodžio.<br>1. Ištrinkite nereikalingas kopijas ir jų DNS įrašus.<br>2. Likusias uždarykite slaptažodžiu. | | |
| Vidutinė | **Sertifikatas baigiasi po 8 d.**<br>Jei automatinis atnaujinimas neveiks, lankytojai pamatys „Ryšys nesaugus“.<br>1. Įjunkite automatinį atnaujinimą talpinimo skydelyje. | | |
| Smulki | **Nėra CAA įrašo**<br>Sertifikatą jūsų domenui gali išduoti bet kuri įstaiga.<br>1. Leiskite tik savo sertifikatų teikėją. | | |

| | | |
|---|---|---|
| Smulki | **Domenas be DNSSEC**<br>DNS atsakymų negalima patikrinti, todėl juos lengviau suklastoti.<br>1. Įjunkite DNSSEC registratoriaus skydelyje. | |

## Metodas ir ribos

Patikrinome: pašto įrašus (SPF, DKIM, DMARC), TLS sertifikatą ir protokolus, svetainės antraštes ir viešus failus, subdomenus iš sertifikatų registrų, atviras paslaugas serveryje. Programinės įrangos versijas sutikrinome su NVD ir OSV pažeidžiamumų duomenų bazėmis, palaikymo terminus – su endoflife.date, aktyviai išnaudojamus pažeidžiamumus – su CISA KEV sąrašu.

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

Tai techninė patikra pagal viešai matomus duomenis, o ne teisinė konsultacija, sertifikatas ar auditas. Ji atspindi būseną patikros dieną; to, ko nematyti iš išorės, ji neįvertina. Mūsų atsakomybė ribojama sumokėta kaina.