request( )

DROŠĪBAS IEVAINOJAMĪBU ATKLĀŠANAS POLITIKA

Pēdējo reizi atjaunota: 2024. gada 18. novembrī

Šī Drošības ievainojamību atklāšanas politika ir sagatavota, lai sniegtu tīmekļa vietnes www.request.lv (turpmāk – Vietne) apmeklētājiem un kiberdrošības pētniekiem informāciju par ievainojamību ziņošanas procedūrām, ziņojumu izmantošanas mērķiem un gan ziņotāja, gan Request (turpmāk – Atbildīgā persona) atbildību.

Atbildīgā persona augsti vērtē ētisko hakeru un plašākas drošības kopienas ieguldījumu, palīdzot nodrošināt mūsu sistēmu un datu drošību.

1. Informācija par Atbildīgo personu

Atbildīgā persona par drošības ievainojamību ziņojumu apstrādi ir SIA Request (turpmāk – Request), vienotais reģistrācijas numurs: 40203423105, juridiskā adrese: Stabu iela 109 - 1, Rīga, LV-1009, Latvija, e-pasta adrese: security@request.lv

2. Mērķis un tiesiskais pamats

Šīs politikas mērķis ir noteikt skaidru procesu, kā atbildīgi ziņot par mūsu sistēmu ievainojamībām, lai palīdzētu uzturēt Atbildīgās personas sniegto pakalpojumu drošību un integritāti.

Ievainojamību ziņojumu apstrāde var ietvert personas datus, piemēram, ziņotāja kontaktinformāciju, kas tiks apstrādāta, pamatojoties uz Vispārīgās datu aizsardzības regulas 6. panta 1. punkta f) apakšpunktu – Atbildīgās personas leģitīmās intereses. Tas ietver ziņojumu izskatīšanu, pārvaldīšanu un atklāto ievainojamību risināšanu. Sīkāku informāciju par to, kā mēs izmantojam, glabājam un aizsargājam jūsu personas datus, lasiet mūsu Privātuma politikā.

SECURITY VULNERABILITY DISCLOSURE POLICY

Last updated: November 18, 2024

This Security Vulnerability Disclosure Policy has been prepared to provide users of the website www.request.lv (hereinafter – the Website) and security researchers with information about the procedures for reporting vulnerabilities in our systems, the purposes for which the information is used, and the responsibilities of both the reporter and Request (hereinafter – the Responsible Entity).

The Responsible Entity values the contributions of ethical hackers and the wider security community to help ensure the safety of our systems and data.

1. Information About the Responsible Entity

The Responsible Entity for the processing of security vulnerability disclosures is SIA Request (hereinafter – Request), registration number: 40203423105, legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia, email address: security@request.lv

2. Purpose and Legal Basis

The purpose of this policy is to define a clear process for the responsible disclosure of vulnerabilities in our systems to help maintain the security and integrity of the services provided by the Responsible Entity.

The processing of vulnerability reports may involve personal data, such as the contact information of the reporter, which will be processed on the legal basis of Article 6(1)(f) of the General Data Protection Regulation – Legitimate Interests of the Responsible Entity. This includes responding to, managing, and resolving reported vulnerabilities. For more information about how we use, store and protect your personal data, please see our Privacy Policy.

3. Politikas piemērošanas joma

Šī politika attiecas uz visām Atbildīgās personas tieši piederošām vai pārvaldītām publiski pieejamām sistēmām un pakalpojumiem, tostarp:

- Tīmekļa vietni un tās apakšdomēniem;
- Vietnēm un tīmekļa lietotnēm, ko izstrādājusi un pārvalda Atbildīgā persona.

Šī politika neattiecas uz:

- Trešo pušu pakalpojumiem un platformām, kas integrētas ar mūsu sistēmām;
- Fizisko infrastruktūru un resursiem.

4. Security.txt faili mūsu vietnēs

Vietnēs, kuras pārvalda Atbildīgā persona, ir pieejami security.txt faili – standarta teksta faili, kas sniedz kiberdrošības pētniekiem vieglu veidu, kā atrast kontaktinformāciju drošības ievainojamību ziņošanai.

Security.txt faili ir izvietoti katras vietnes direktorijā /.well-known/. Piemēram, vietnes www.request.lv security.txt failu var atrast saitē www.request.lv/.well-known/security.txt

Šie faili satur:

- Kontaktinformāciju drošības ievainojamību ziņošanai;
- Vēlamo valodu sarakstu drošības ievainojamību ziņošanai;
- Security.txt faila derīguma termiņu;
- Saiti uz šo Drošības ievainojamību atklāšanas politiku;
- Papildu resursus, piemēram, mūsu PGP (Pretty Good Privacy) publisko šifrēšanas atslēgu drošai saziņai.

Mēs iesakām pētniekiem atsaukties uz security.txt failu, lai iegūtu visjaunāko informāciju par drošības ievainojamību ziņošanu.

3. Scope of the Policy

This policy applies to all publicly accessible systems and services directly owned or operated by the Responsible Entity, including:

- The Website and its subdomains;
- Websites and web applications developed and managed by the Responsible Entity.

The following are outside the scope of this policy:

- Third-party services and platforms integrated with our systems;
- Physical infrastructure and non-digital assets.

4. Security.txt Files on Our Websites

Websites managed by the Responsible Entity contain a security.txt file, a standard text file designed to provide security researchers with an easy way to find our vulnerability disclosure contact details.

The security.txt file is located in the /.well-known/ directory of every website. For example, the security.txt file for www.request.lv can be found at www.request.lv/.well-known/security.txt

These files contain:

- Contact information for reporting security vulnerabilities;
- List of preferred languages for security vulnerability disclosures;
- Expiration date and time of the security.txt file;
- Link to this Security Vulnerability Disclosure Policy;
- Additional resources, such as our PGP (Pretty Good Privacy) public encryption key, for secure communication.

We encourage researchers to refer to the security.txt file for the most up-to-date information on reporting security vulnerabilities.

5. Aizliegtās testēšanas metodes

Ir stingri aizliegts izmantot šādas testēšanas metodes:

- Veikt sociālās inženierijas uzbrukumus;
- Automatizēti minēt sistēmu un/vai lietotāju paroles (brute-forcing);
- Izmantot ievainojamības, lai iegūtu, modificētu vai dzēstu informāciju;
- Mēģināt ietekmēt pakalpojumu pieejamību ar pakalpojuma atteices (DoS vai DDoS) uzbrukumiem;
- Izmantot ievainojamības, lai piekļūtu sensitīvai informācijai (izņemot minimāli nepieciešamo apjomu, lai pierādītu ievainojamības esamību).

Ja testēšanas laikā jūs sastopaties ar šāda veida informāciju, jums nekavējoties jāpārtrauc testēšana un jāziņo par atklājumu Atbildīgajai personai:

- Personas identificējošu informāciju;
- Komercnoslēpumus vai patentētu informāciju;
- Finanšu informāciju, piemēram, bankas kontu vai norēķinu karšu / kredītkaršu datus.

6. Ziņošana par ievainojamību

Lai ziņotu par ievainojamību, lūdzu, sazinieties ar mūsu drošības incidentu reaģēšanas komandu, rakstot uz e-pastu security@request.lv

Ja jūsu ziņojumā ir ietverta sensitīva informācija, mēs iesakām izmantot PGP (Pretty Good Privacy) šifrēšanu. Mūsu publisko PGP šifrēšanas atslēgu var iegūt saitē www.request.lv/lv/drosiba

Iesniedzot ziņojumu, lūdzu, norādiet:

- Detalizētu atklātās ievainojamības aprakstu, tostarp tās atveidošanas soļus;
- Atklātās ievainojamības darbības jomu, piemēram, skartās sistēmas vai datus;

5. Prohibited Testing Methods

The following testing methods are strictly prohibited:

- Performing social engineering attacks;
- Automated brute-forcing or guessing of system and/or user passwords;
- Exploiting vulnerabilities to extract, modify, or delete information;
- Attempting to impact service availability through denial-of-service (DoS or DDoS) attacks;
- Exploiting vulnerabilities to access sensitive information (except the minimal amount necessary to demonstrate the vulnerability's existence).

If during testing you encounter any of the following types of information, you must stop testing immediately and report the finding to the Responsible Entity:

- Personally identifiable information;
- Trade secrets or proprietary information;
- Financial information, such as bank account or debit card / credit card details.

6. Reporting a Vulnerability

To report a vulnerability, please contact our security incident response team via email at security@request.lv

If your report contains sensitive information, we encourage the use of PGP (Pretty Good Privacy) encryption. Our public PGP encryption key can be retrieved at www.request.lv/security

When submitting your report, please include:

- A detailed description of the discovered vulnerability, including steps to reproduce it;
- The scope of the discovered vulnerability, such as the affected systems or data;

- Jebkādus atbalstošus pierādījumus, piemēram, ekrānuzņēmumus vai koncepcijas kodu;
- Jūsu kontaktinformāciju jautājumu uzdošanai ziņojuma pārskatīšanas un izmeklēšanas laikā.

7. Atbildīgās personas apņemšanās

Atbildīgā persona neuzsāks tiesiskas darbības pret personām, kuras:

- Ievēro šo politiku ievainojamību testēšanas un ziņošanas laikā;
- Ievēro savas dzīvesvietas valsts un Latvijas Republikā piemērojamos likumus;
- Atturas no ievainojamību detaļu publiskas atklāšanas, pirms Atbildīgā persona ir izmeklējusi un atrisinājusi problēmu.

8. Nobeiguma jautājumi

Šī Drošības ievainojamību atklāšanas politika pēc nepieciešamības var tikt mainīta, aktuālajai politikas versijai tiekot publicētai Request tīmekļa vietnē.

Šī Drošības ievainojamību atklāšanas politika ir pieejama Request tīmekļa vietnē arī angļu valodas versijā (www.request.lv/security/vulnerability-disclosure-policy). Neatbilstību vai pretrunu gadījumā starp latviešu un angļu valodas versijām, latviešu valodas versija (www.request.lv/lv/drosiba/ievainojamibu-atklasanas-politika) būs noteicošā visos aspektos.

Jautājumu gadījumā par šo politiku vai ievainojamību ziņošanas procesu ar Atbildīgo personu var sazināties nosūtot ierakstītu vēstuli uz uzņēmuma juridisko adresi: Stabu iela 109 – 1, Rīga, LV-1009, Latvija vai e-pastā: security@request.lv

Apstiprinu:

D. Bethers
Valdes loceklis

- Any relevant supporting evidence, such as screenshots or proof-of-concept code;
- Your contact information for follow-up questions during the review and investigation of the report.

7. Responsible Entity Commitments

The Responsible Entity will not take legal action against individuals who:

- Comply with this policy during their testing and reporting of vulnerabilities;
- Adhere to applicable laws in their country of residence and the Republic of Latvia;
- Refrain from disclosing vulnerability details publicly before the Responsible Entity has investigated and resolved the issue.

8. Closing Remarks

This Security Vulnerability Disclosure Policy may be amended as necessary, with the current version of the policy being published on the Request website.

This Security Vulnerability Disclosure Policy is also available on the Latvian language version of the Request website (www.request.lv/lv/drosiba/ievainojamibu-atklasanas-politika). In the event of any inconsistency or conflict between the English and Latvian versions, the Latvian version (www.request.lv/lv/drosiba/ievainojamibu-atklasanas-politika) shall prevail in all respects.

In case of any questions regarding this policy or the processing of vulnerability disclosures, you can contact the Responsible Entity by sending an official letter to the company's legal address: Stabu iela 109 - 1, Riga, LV-1009, Latvia or by email: security@request.lv

Approved:

D. Bethers
Board Member