SADEINNOVATIONS

KOORDINOIDUN HAAVOITTUVUUKSIEN JULKISTAMISEN POLITIIKKA

COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY

SADE Innovations Oy · Versio 1.0 · Approved

KOORDINOIDUN HAAVOITTUVUUKSIEN JULKISTAMISEN POLITIIKKA

Tämä dokumentti kuvaa, miten SADE Innovations Oy ("me", "yhtiö") vastaanottaa, käsittelee ja korjaa tuotteissamme ja palveluissamme havaittuja tietoturvahaavoittuvuuksia. Politiikka on laadittu EU:n kyberkestävyysasetuksen (Cyber Resilience Act, CRA, asetus (EU) 2024/2847) liitteen I osan II ja artiklan 13(8) vaatimusten mukaisesti.

1. TARKOITUS

Tämän politiikan tavoitteena on tarjota tietoturvatutkijoille, asiakkaillemme, yhteistyökumppaneillemme ja muille tahoille selkeä ja turvallinen tapa ilmoittaa meille löytämistään tietoturvahaavoittuvuuksista, sekä kuvata prosessi, jolla käsittelemme näitä ilmoituksia vastuullisesti.

2. SOVELTAMISALA

Tämä politiikka koskee seuraavia SADE Innovations Oy:n tuotteita, palveluita ja rajapintoja:

- Booster Pilvipalvelu
- Booster Web-sovellus
- Booster Mobiilisovellus
- Booster ESP
- Booster nRF Connect
- Booster OS + Edge Node

Politiikka koskee myös tilanteita, joissa haavoittuvuus havaitaan ratkaisumme integroineen kumppaniyrityksen tuotteessa tai sen loppukäyttäjän laitteessa, mikäli haavoittuvuus juontuu SADE Innovations Oy:n toimittamasta komponentista.

2.1 SOVELTAMISALAN ULKOPUOLELLA

- Sosiaalisen manipuloinnin (social engineering) testaus henkilöstöämme kohtaan
- Fyysinen tunkeutuminen toimitiloihimme
- Palvelunestohyökkäykset (DoS/DDoS) ilman erillistä ennakkolupaa
- Kolmansien osapuolten omistamat järjestelmät, joita emme hallinnoi

3. MITEN RAPORTOIDA HAAVOITTUVUUS

Ilmoita havaitsemasi haavoittuvuus sähköpostitse osoitteeseen:

security@sadeinnovations.com

Pyydämme sisällyttämään ilmoitukseen mahdollisuuksien mukaan seuraavat tiedot:

- Haavoittuvuuden kuvaus ja arvioitu vaikutus
- Askel askeleelta -ohjeet haavoittuvuuden toistamiseksi
- Kyseinen tuote, versio tai järjestelmä

- Mahdollinen proof-of-concept (PoC) tai muu tekninen todiste
- Yhteystietosi (jos toivot vastausta tai haluat tulla mainituksi kiitoksissa)

Otamme vastaan myös anonyymit ilmoitukset. Emme kuitenkaan tällöin pysty vahvistamaan ilmoituksen vastaanottoa tai antamaan päivityksiä ilmoittajalle.

4. KÄSITTELYPROSESSI JA AIKATAULU

- Kuittaus: vahvistamme ilmoituksen vastaanoton [2] arkipäivän kuluessa.
- Arviointi: arvioimme ja luokittelemme haavoittuvuuden vakavuuden (CVSS-pohjaisesti) [10] arkipäivän kuluessa.
- Korjaus: kehitämme ja validoimme korjauksen vakavuusluokituksen mukaisella aikataululla — kriittiset haavoittuvuudet [7] vuorokaudessa, muut porrastetusti.
- Julkistus: julkaisemme tiedon haavoittuvuudesta vasta korjauksen ollessa saatavilla, ellei toisin sovita ilmoittajan kanssa. Oletusarvoinen tavoiteaika julkistukselle on [90] päivää ilmoituksesta.

Pidämme ilmoittajan tietoisena etenemisestä koko prosessin ajan, mikäli yhteystiedot on annettu.

5. VASTUULLISEN RAPORTOINNIN LUPAUS (SAFE HARBOR)

Emme ryhdy oikeustoimiin hyvässä uskossa toimivaa tietoturvatutkijaa vastaan, mikäli tämä:

- noudattaa tätä politiikkaa ja pysyy soveltamisalan (kohta 2) rajoissa,
- ei julkista tietoa haavoittuvuudesta ennen kuin korjaus on saatavilla tai olemme yhdessä sopineet julkistamisajankohdasta,
- ei käytä haavoittuvuutta muuhun kuin sen olemassaolon todentamiseen (esim. ei käytä sitä datan poimimiseen tai järjestelmien vahingoittamiseen).

6. TUKIJAKSO JA TIETOTURVAPÄIVITYKSET

Sitoudumme tarjoamaan tietoturvapäivityksiä kattamillemme tuotteille vähintään [5] vuoden ajan tuotteen markkinoille saattamisesta, tai tuotteen ilmoitetun elinkaaren loppuun asti, CRA:n vaatimusten mukaisesti.

7. YHTEYS KANSALLISEEN KOORDINAATTORIIN

Mikäli et saa meihin yhteyttä tai haavoittuvuus koskee useampaa toimijaa, voit vaihtoehtoisesti olla yhteydessä Suomen kansalliseen kyberturvallisuuden koordinointielimeen:

- Traficom / Kyberturvallisuuskeskus (NCSC-FI) — vulncoord@traficom.fi

8. POLITIIKAN PÄIVITTÄMINEN

Tätä politiikkaa tarkistetaan ja päivitetään säännöllisesti. Viimeisin päivitys: 25.09.2026.

COORDINATED VULNERABILITY DISCLOSURE (CVD) POLICY

This document describes how SADE Innovations Oy ("we", "the company") receives, handles and remediates security vulnerabilities identified in our products and services. This policy has been prepared in accordance with the requirements of the EU Cyber Resilience Act (CRA, Regulation (EU) 2024/2847), Annex I Part II and Article 13(8).

1. PURPOSE

The purpose of this policy is to provide security researchers, customers, partners and other parties with a clear and safe way to report security vulnerabilities they discover, and to describe the process by which we handle such reports responsibly.

2. SCOPE

This policy applies to the following SADE Innovations Oy products, services and interfaces:

- Booster Cloud
- Booster Web App
- Booster Mobile App
- Booster ESP
- Booster nRF Connect
- Booster OS + Edge Node

This policy also applies where a vulnerability is identified in a partner company's product that integrates our solution, or in an end user's device, where the vulnerability originates from a component supplied by SADE Innovations Oy.

2.1 OUT OF SCOPE

- Social engineering testing against our staff
- Physical intrusion into our premises
- Denial-of-service (DoS/DDoS) testing without prior written approval
- Systems owned by third parties that we do not control

3. HOW TO REPORT A VULNERABILITY

Please report any vulnerability you discover by email to:

security@sadeinnovations.com

Where possible, please include:

- A description of the vulnerability and its estimated impact
- Step-by-step instructions to reproduce the issue
- The affected product, version or system
- Any available proof-of-concept (PoC) or other technical evidence

- Your contact details (if you would like a response or wish to be credited)

We also accept anonymous reports. In that case, we will not be able to confirm receipt or provide status updates to the reporter.

4. HANDLING PROCESS AND TIMELINES

- Acknowledgment: we confirm receipt of the report within [2] business days.
- Assessment: we assess and classify the severity of the vulnerability (CVSS-based) within [10] business days.
- Remediation: we develop and validate a fix on a timeline based on severity — critical vulnerabilities within [7] days, others on a staged schedule.
- Disclosure: we publish information about the vulnerability only once a fix is available, unless otherwise agreed with the reporter. The default target for disclosure is [90] days from the report.

We keep the reporter informed of progress throughout the process, where contact details have been provided.

5. SAFE HARBOR COMMITMENT

We will not pursue legal action against a security researcher acting in good faith who:

- follows this policy and stays within the defined scope (Section 2),
- does not disclose information about the vulnerability before a fix is available or before we have jointly agreed on a disclosure date,
- does not use the vulnerability for any purpose beyond verifying its existence (e.g. does not exfiltrate data or damage systems).

6. SUPPORT PERIOD AND SECURITY UPDATES

We commit to providing security updates for covered products for at least [5] years from the date the product is placed on the market, or until the end of its stated support period, in accordance with CRA requirements.

7. NATIONAL COORDINATOR CONTACT

If you are unable to reach us, or if the vulnerability affects multiple parties, you may alternatively contact Finland's national cybersecurity coordination body:

- Traficom / National Cyber Security Centre Finland (NCSC-FI) — vulncoord@traficom.fi

8. POLICY UPDATES

This policy is reviewed and updated periodically. Last updated: 25.09.2026.