Danke Solar, LLC, Vulnerability Disclosure Policy

Effective Date: June 18, 2025

Introduction

Danke Solar is committed to ensuring the security of its users and customers by protecting their information. This policy is intended to give security researchers clear guidelines for escalating discovered vulnerabilities and to convey our procedures for submitting relevant findings to us.

This policy describes **what systems and types of research** are covered under this policy, **how to deliver** vulnerability reports, and **how long** we ask security researchers to wait before publicly disclosing vulnerabilities.

We encourage you to contact us to report potential vulnerabilities in our systems.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized and we will work with you to understand and resolve the issue quickly. Danke Solar will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

Under this policy, "research" means activities in which you:

- Notify us as soon as possible after you discover a practical concern or potential security issue.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems.
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly. See the timeline section below.
- Please do not submit a high volume of low-quality reports as this will delay our ability to properly assess.

Once you've established that vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), **you must stop your test, notify us immediately, and not disclose this data to anyone else**.

Test Methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Reporting Vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely Sunnova, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission. To ensure information security when reporting vulnerabilities, we will only accept vulnerability reports that are encrypted using **Danke Solar Pretty Good Privacy (PGP) Key**. Danke Solar Public Key is located below:

Copy PGP Key

What We Would Like to See From You

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location where vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- We prefer all reports to be submitted in English.

What you can expect from us

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 5 business days, we will acknowledge that your report has been received.
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as legally and technically prudent about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution

Timelines for Public Statement

Sunnova requests a press embargo for a minimum of 30 days with or without issue resolution or response, using the submission date as the first day. Further, Sunnova requests that if we have acknowledged to the reporter the submission and are engaged, this embargo be set at 90 days.

Questions:

Questions regarding this policy may be sent to [appropriate email address]

Document Change History

Version: 6182025-1.0
Date: June 18, 2025
Description: First Issuance
Date: Juen 18, 2025
Description: Reporting a Vulnerability