Responsible Disclosure Policy

Version : 1.1

Date : 17/03/2022

Auteur : CERT TotalEnergies

PURPOSE

This Responsible Disclosure Policy, established by TotalEnergies CERT, sets out the framework and procedure for alerting us if you have discovered one or more vulnerabilities in our computer systems and networks (websites, mobile applications, etc.).

This Responsible Disclosure Policy is not a “Bug Bounty” Program. The public is not encouraged or allowed to actively search for vulnerabilities in TotalEnergies systems and networks (web, app, etc.).

This Responsible Disclosure Policy does not apply to TotalEnergies licensors and providers. Indeed, because of the existing contractual relationships, they must follow the specific stipulations provided for this purpose.

CONTACT

Vulnerability disclosures must be sent by using the form in https://vdp.totalenergies.com.

For all other subjects, the CERT TotalEnergies can be reached by email, into English or French, to contact@cert.total.

In order to ensure confidentiality of the exchanges, it is strongly recommended to encrypt your emails using our PGP key available here: https://www.totalenergies.com/cert.

PERSONAL DATA / ANONYMITY

- You can contact us using means that ensure your anonymity and/or by using a pseudonym.
- You may provide us with your IP address, which would have been recorded by our systems, when you discovered the vulnerability in order to exclude yourself from the list of potential hackers.
- You must limit the sending of personal or sensitive data to what is necessary to understand or solve the reported vulnerability.

- As part of the Responsible Disclosure Policy, and in accordance with the applicable laws and regulations relating to the protection of personal data, the TotalEnergies CERT, in its capacity of data controller, carries processing of personal data you voluntarily provided (e.g. IP address, email address, contact details, etc.) for the purpose of managing your vulnerabilities' alerts and exclude you from the list of potential hackers, on the basis of your consent and TotalEnergies CERT's legitimate interest.

Your data will not be stored for longer than is needed to fulfill the purpose of the processing. In the event of legal or administrative action on the vulnerabilities, they will be retained for the duration of action. In accordance with the current regulations, you have the right to access, correct, delete your data. To exercise your rights and ask us about the processing of your persona data, you can email contact@cert.total. If, after contacting us, you believe that your rights have not been respected, you may submit a complaint to the competent supervisory authority.

WHAT YOU SHOULD DO

- Contact us as soon as possible after discovering a vulnerability in our systems or networks (web, apps, etc.).
- Comply with all applicable laws and regulations.
- Try to provide us with enough information so that we can identify, reproduce and solve the vulnerability. We may ask you for further details or information.
- Be careful to maintain the confidentiality of any information you may have had access to when discovering the vulnerability(ies) and during our exchanges.

WHAT YOU CANNOT DO

- Do not make public the discovered vulnerability(ies) affecting TotalEnergies, including if the vulnerability(ies) is (are) already publicly known (unrelated to TotalEnergies), and do not share it (them) with third parties unless required to do so by the applicable law and only to the extent of such legal requirements;
- Limit your exposure to any vulnerabilities you may have discovered, including avoiding downloading data accessible through the vulnerability, investigating or staying on systems and networks made accessible through the vulnerability, or modifying data on them.
- Do not test or use any means or services to discover possible vulnerabilities in our systems and networks, through DDOS attacks, port scans, phishing, ransomware, etc.

- Do not disclose to a third party any information relating to the vulnerability discovered and reported to TotalEnergies or the information made accessible through this vulnerability.

TOTALENERGIES :

- We will acknowledge your report within a reasonable time.
- We will handle your report with strict confidentiality.
- Where possible, we will inform you of the resolution of the vulnerability you have reported to us.
- We may contact you again to ask for additional information that allows us to properly address and remedy the vulnerability.

TotalEnergies will not take any legal action against persons who act in good faith, in accordance with the instructions and guidelines outlined in this Responsible Disclosure Policy and the applicable laws.

COMPENSATION, RETRIBUTION:

No compensation or retribution will be due or may be required. However, TotalEnergies remains free to grant a reasonable gratification, on an exceptional basis, especially in view of the importance of the vulnerability discovered.

TotalEnergies makes reasonable efforts to process reports but it will not be liable to you for the processing or failure to process your report, including our failure to acknowledge receipt of your report or to respond to your messages.

END OF THE POLICY