PSIRT responsible handling policy

At Texas Instruments (TI), we set a high priority on the security of our products; however, as we all know, no matter how much effort is put into product security, no product or customer system can be 100% secure.

The TI Product Security Incident Response Team (PSIRT) wants to learn about any potential security issues impacting our products so we can take the necessary steps to promptly address them.

We appreciate the security community's work and recognize the crucial role its members play in helping to improve product security. It is our goal to foster an open and mutually beneficial collaboration with security researchers. Below are our thoughts and expectations on how we can work together to achieve that goal.

What you can expect from us

- ***Responsiveness*** – we will respond to your communications in a timely manner.
- ***Transparency*** – we will keep you informed of our progress towards resolving the reported incident; specifically, we will update you on the status of the potential vulnerability as we complete each stage of our incident response process.
- ***Responsible handling of information*** – we will not publicly disclose the contents of your findings without coordinating with you. Should security considerations require we share critical portions of your findings with other stakeholders (e.g. customers), we will first inform you and explain our reasoning before sharing. When appropriate, we will coordinate with you on an embargo (i.e. a time period during which neither of us will disclose incident details to others).
- ***Fairness*** – as the incident response process reaches a close, we will coordinate with you on issuing a security advisory if we determine it is appropriate. If we publish a security advisory, we typically acknowledge you and your team for your findings. At this time, we do not offer a bug bounty program.

What we expect from you

- ***Responsiveness*** – we ask for timely responses to our communications, as this will help us move more quickly to resolve your incident report.
- ***Transparency*** – in order to verify and address potential security vulnerabilities, we ask you to be open with us regarding your findings and your plans for public disclosure.
- ***Responsible handling of information*** – we trust that you will not publicly disclose your findings with other stakeholders (e.g. TI customers or business partners) without prior coordination with us at least two weeks ahead of our agreed-upon embargo. Even if there is not an embargo in effect, we ask for a two-week notice before any information is disclosed publicly or among internal audiences.

  Premature disclosure or sharing incomplete information can lead to misunderstanding and increase the risk to potentially impacted parties. By providing us with two-week notice before any disclosure, we can ensure the accuracy of information shared.
- ***Fairness*** – in order to work effectively to address issues and reduce the risk to potentially impacted parties, we ask that you reciprocate our approach and attitude toward you, and that you treat us fairly and respectfully. We share a common goal of improving product security and minimizing the impact of security

incidents on companies and the general public. This common goal creates the foundation for a respectful working relationship.

How to submit a vulnerability report

To submit a vulnerability report in line with this policy to TI's PSIRT, please visit the TI PSIRT website.

For potential vulnerabilities involving open source software (OSS) used in TI products, please refer to the security vulnerability handling and advisory websites of the corresponding OSS developer, if available, to review their handling policy and status of the vulnerability fixes.

TI will follow its PSIRT process for TI authored software, contributions or customizations to OSS used in its products.