PSIRT responsible handling policy

TEXAS INSTRUMENTS

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 percent secure.

TI wants to learn about any potential security issues impacting our products so that we can take the necessary steps to promptly address them. We recognize and 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. We want to share 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 send a notification of the status of the potential vulnerability when we complete each stage of our incident response process.
- ***Responsible handling of information*** – we respect the need for you to be able to share information with us without concern it will be prematurely made public; we will not publicly disclose the contents of your report without coordinating with you. Where security considerations require sharing critical portions of your report with selected other stakeholders (e.g. customers), we will 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 comes to a close, we will coordinate with you to make a public disclosure of the incident as appropriate. We will give you and your team recognition for your efforts.

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 disclosure and public communication.
- ***Responsible handling of information*** – we trust you will not publicly disclose your reported information or share it with other stakeholder (e.g. TI customers or business partners) without previously coordinating with us. Premature public disclosure can undermine the effectiveness of our mutual goals, as incomplete or inaccurate information leads to misunderstanding and can increase risk for potentially impacted parties. And we trust that you will respect any agreed-upon embargo.
- ***Fairness*** – in order to work effectively to address issues and reduce risk for potentially affected parties, we ask that you reciprocate our approach and attitude toward you, and that you treat us fairly and with respect. We share common goals of improving security and minimizing the impact of incidents on companies and the public. Those common goals create 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 Product Security Incident Response Team (PSIRT), please visit the TI PSIRT website and follow the instructions given there.