Vulnerability Disclosure Policy

A Lattice Semiconductor Security Document

August 2026

Report security issues:
security@latticesemi.com

Introduction

Lattice Semiconductor welcomes feedback from security researchers, customers, partners, and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issue in any of our assets, we want to hear from you. This policy outlines how to report vulnerabilities to us, what we expect, and what you can expect from us.

Systems in Scope

This policy applies to Lattice products with digital elements and associated digital infrastructure.

Out of Scope

Products not manufactured or supplied by Lattice, including third-party products used in the same system as a Lattice product, are out of scope.

Vulnerabilities discovered or suspected in out-of-scope systems should be reported to the appropriate vendor or authority.

Our Commitments

When working with us under this policy, you can expect us to:

- Respond to your report promptly and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed, and
- Work to remediate confirmed vulnerabilities in a timely manner, within our operational constraints.

Rules of Engagement

If you participate in our vulnerability disclosure program in good faith, we ask that you:

- Follow this policy and any other applicable agreements;
- Report suspected vulnerabilities promptly through the Official Channels identified below;
- Perform testing only on systems, hardware, software installations, and accounts that you own or are explicitly authorized to test;
- Do not perform social engineering, phishing, or physical attacks against Lattice employees, contractors, offices, customers, or users;
- Do not perform denial-of-service attacks or load, stress, or resource-exhaustion testing against Lattice-operated services, production infrastructure, or other live systems;
- You may report denial-of-service or availability weaknesses in Lattice products. Testing of these conditions must be limited to hardware, software, and test environments that you own or are explicitly authorized to use;
- Avoid disrupting systems, degrading availability, destroying or modifying data, violating the privacy of others, or harming the user experience;
- If you obtain unintended access to a system, account, or data, stop at the point of recognition. Access only the minimum information necessary to demonstrate the issue. Do not attempt to determine what additional information may be accessible, and report the issue immediately;
- Interact only with test accounts that you own or accounts for which the account holder has provided explicit permission;
- If you encounter personal, health, payment card, confidential, or proprietary information, stop testing and report the issue immediately;
- Give Lattice a reasonable opportunity to investigate and address the issue before public disclosure;

- Do not sell, trade, transfer, or use information about the vulnerability for any purpose other than reporting it to and coordinating with Lattice; and
- Do not engage in extortion.

Official Channels

Please report security issues to security@latticesemi.com, providing all relevant information. The more detail you provide, the easier it will be for us to triage and fix the issue.

Encryption (PGP)

For sensitive reports, please encrypt your message using our PGP public key below.

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEapi01hYJKwYBBAHaRw8BAQdAq/oUErI87Pf39PSzkNhLjvE5g0+EsTwsNr/g
2B23DrW0WExhdHRpY2UgU2VtaWNvbmR1Y3RvciBQcm9kdWN0IFNlY3VyaXR5IElu
Y2lkZW50IFJlc3BvbnNlIFRlYW0gPHNlY3VyaXR5QGxhdHRpY2VzZW1pLmNvbT6I
tQQTFgoAXRYhBFX2fC/WrsrPqc4X6wXhREma35zcBQJqmLTWGxSAAAAAAAQADm1h
bnUyLDIuNSsxLjEyLDIsMQIbgQUJBaSpWgULCQgHAgIiAgYVCgkICwIEFgIDAQIe
BwIXgAAKCRAF4URJmt+c3Ml9APsGJUVkfOtuy9+SfGUqb4sYksZ4u5Z8IB6NoZ/5
J8FlogEA2aIhOTSrRPmI7het3IgaIhpk7zMNUWBeYgiwv+mTUw+4MwRqmLT0Fgkr
BgEEAdpHDwEBB0DITN3ltDIiA88G4sh/bAgAJSHIlYdmuKcb7k959N3inokBCwQY
FgoAPBYhBFX2fC/WrsrPqc4X6wXhREma35zcBQJqmLT0GxSAAAAAAAQADm1hbnUy
LDIuNSsxLjEyLDIsMQIbAgCBCRAF4URJmt+c3HYgBBkWCgAdFiEELehoZ6geLPeU
YjsqF/w3rbLSh7QFAmqYtPQACgkQF/w3rbLSh7TpsAD+Jf0m9PzLeCt8vvDuWT3y
TQgLbUEWVPfhTXd3I386El0BALxY/GVzH1058bhN2c7lqS6fz4pD7NfhHR3OINoZ
mD8OzsUA/2P7iTIpFdpN6LUSaSUIEUOVsYaz0hX2LiIPKZKTXQg8AP90bjr4awAS
lNwX98v5v/zBIX9OpoJ5Yv9lUNvV8C96Bg== =1w0o

-----END PGP PUBLIC KEY BLOCK-----