Notice of Vulnerability Disclosure Policy (VDP) Ciena and Blue Planet

Introduction

Ciena (NYSE: CIEN) is a global leader in networking systems, services, and software. We build the most adaptive networks in the industry, enabling customers to anticipate and meet ever-increasing digital demands. For three-plus decades, Ciena has brought our humanity to our relentless pursuit of innovation. Prioritizing collaborative relationships with our customers, partners, and communities, we create flexible, open, and sustainable networks that better serve all users—today and into the future.

This Notice of Vulnerability Disclosure Policy (VDP) sets forth the reporting and disclosure process that Ciena and its Blue Planet division (collectively, "Ciena") follow when we receive vulnerability reports.

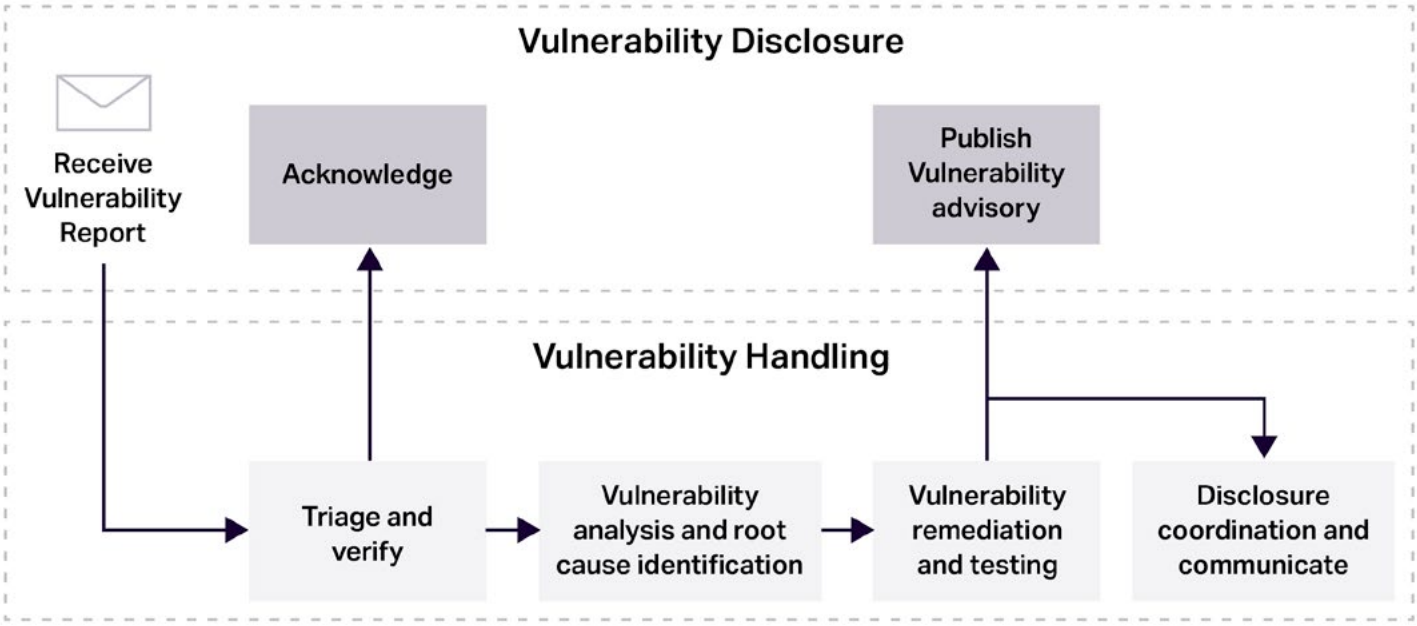
We have established this Notice of Vulnerability Disclosure Policy (VDP) to facilitate the responsible reporting of security vulnerabilities in our products and services. The security of our products and services is of paramount importance to us. We are committed to providing secure and reliable solutions that meet the highest standards of quality and performance. We are also concerned about the potential impact of security vulnerabilities on our customers and their end-users.

The VDP outlines the scope, process, and expectations for reporting security vulnerabilities to us, as well as our commitments and responsibilities to you as a reporter. We appreciate your cooperation and collaboration in helping us protect our customers and their networks.

To ensure the security of our products and services, we have established a dedicated Product Security Incident Response Team (PSIRT) that is responsible for responding to cyber incidents and vulnerability reports affecting Ciena's products and services. The PSIRT is composed of security experts from different functions within Ciena, such as engineering, product management, customer support, legal, communications, and sales. The PSIRT operates 24/7/365 and follows industry best practices and standards for vulnerability handling and disclosure.

Vulnerability handling and disclosure process

The PSIRT aligns with the ISO/IEC 30111 standard for vulnerability handling processes and the ISO/IEC 29147 standard for vulnerability disclosure. These standards provide guidelines for how organizations should receive, investigate, remediate, disclose, and communicate security vulnerabilities in their products or services. The PSIRT also follows the principles of coordinated vulnerability disclosure (CVD), which is a collaborative approach between the reporter and the vendor to share information and work together to resolve the vulnerability in a timely manner.



Reporting a vulnerability

Information submitted under this policy will be used for defensive purposes only – to mitigate or remediate vulnerabilities. If reported findings include newly discovered vulnerabilities affecting all users of a product or service, Ciena may share finding information with the appropriate security agencies for handling under the coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports via psirt@ciena.com. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 7 calendar days.

What we would like to see from you

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

- Describe where and how the vulnerability was discovered and the potential impact of the exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts or screenshots are helpful).
- Be in English, if possible.

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 7 calendar days, we will acknowledge that your report has been received.
- Upon completing our investigation and analysis, we will notify you if a Common Vulnerabilities and Exposures (CVE) will be published.
- We will maintain an open dialogue to discuss issues.

Scope

This VDP applies to the products and services that are owned, operated, manufactured, or maintained by Ciena or Blue Planet. The following products and services are **out of scope** for this VDP:

- Third-party components and vulnerabilities found in systems from our vendors fall outside of this policy's scope. We are interested to learn about vulnerabilities that may impact our products and services, and we may assist in reporting to the third party.

We ask that you avoid any activities that could cause harm or damage to our systems, services, customers, or third parties.

If you aren't sure whether a system is in scope or not, contact us at psirt@ciena.com **before starting your research.**

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the **scope** and the **guideline** sections of this document. If there is a particular system not in scope that you think merits testing, please contact us to discuss it first. We may increase the scope of this policy over time. We reserve the right to modify the scope of this VDP at any time without prior notice. Please check this VDP regularly for any updates or changes.

Please note that Ciena and Blue Planet do not offer any monetary rewards or bounties for reporting vulnerabilities under this VDP. However, we may provide recognition by including the researcher's name (with consent) in our product vulnerability advisories or acknowledgments page once the vulnerability is disclosed and fixed. We appreciate your understanding and cooperation in this matter.

Guidelines and safe harbor

We value the contributions of security researchers and ethical hackers who help us improve the security of our products and services. We do not want to discourage or hinder anyone from reporting vulnerabilities to us in a responsible manner. Therefore, we provide a safe harbor for those who comply with this VDP and act in good faith.

This means that we will not pursue legal action against you or ask law enforcement to investigate you if you report a vulnerability to us as long as you:

1. Follow the rules and scope of this VDP.
2. Avoid accessing, modifying, or deleting any data that does not belong to you.
3. Avoid causing any damage or disruption to our systems or services.
4. Avoid violating the privacy or rights of our customers, employees, or third parties.
5. Do not disclose any vulnerability details to anyone else until we confirm that it is fixed or that we agree on a coordinated disclosure timeline.
6. Provide us with a reasonable amount of time to fix the vulnerability before making any public disclosure.
7. Once you've established that a vulnerability exists or encounter any sensitive data (including personally identifiable information, financial information, proprietary information, or trade secrets of any party), **you must stop your test, notify Ciena immediately, and not disclose this data to anyone else.**

We consider these actions to be a demonstration of your good faith and your intention to help us improve our security posture. However, if you engage in any malicious or unlawful activities that are outside the scope of the rules of this VDP, you will lose the protection of this safe harbor agreement.

We also reserve the right to modify the terms of this safe harbor at any time without prior notice. Please check this VDP regularly for any updates or changes.

CVE Publication

We follow the principles of responsible disclosure, and we expect the same from the individuals or organizations who report vulnerabilities to us. This means that we ask you to refrain from publicly disclosing any vulnerability details until we confirm that it is fixed or that we agree on a coordinated disclosure timeline.

We do our best to publicly disclose the vulnerabilities that are reported under this Notice of Vulnerability Disclosure Policy (VDP) in our products and services, as well as acknowledging the researchers who reported them to us (with consent). We do this by publishing product vulnerability advisories on our website and assigning Common Vulnerabilities and Exposures (CVE) identifiers to the vulnerabilities. CVE is a list of publicly disclosed vulnerabilities that provides a standardized reference method for publicly known information security vulnerabilities and exposures.

Contacts and questions

Questions regarding this policy may be sent to psirt@ciena.com. We also invite you to contact us with suggestions for improving this policy.

For customers or partners, we recommend contacting us via your my.ciena.com account.

Privacy

We respect the privacy of vulnerability reporters, and we are committed to protecting their personal information in accordance with applicable laws and policies.

When you report a vulnerability to us, you may choose to provide your name and contact information, or you may report anonymously. We will use your personal information only for the purpose of communicating with you about the vulnerability report and its resolution. We will not share your personal information with any third parties without your consent unless required to by law or for security reasons. For more information, please see our Privacy Notice.