INFOBRIEF

Ciena product security analysis and vulnerability reporting process

The triage and reporting of vulnerabilities associated with Ciena's portfolio is critical to properly manage risk to Ciena and Ciena's customers, providing consistent guidance and experiences. The characteristics of this process have the following attributes:

- Consistent
- Repeatable
- Scalable
- Transparent

This process defines how vulnerabilities are identified, triaged, and tracked. The process further defines the inbound and outbound communication processes with which all Ciena products and services will comply. Objectives include aligning to internationally recognized standards ISO/IEC 30111 (information technology, security techniques, vulnerability handling processes) and ISO/IEC 29147 (information technology, security techniques, vulnerability disclosure).

This process is only used for products that have reached general availability (GA) and are exposed to our customers. Products in development, but not available to outside organizations or customers, are to follow the secure development processes defined elsewhere.

The defined analysis and reporting process includes the following steps:

1. A vulnerability is published and shared in industry or discovered internally. (See next page for contact information.)
2. The Common Vulnerability Scoring System (CVSS) score is reviewed to set likely expectations and urgency from the customer.
3. Ciena will conduct our assessment of impact.
4. It will be determined if the vulnerability:
   a. Is Ciena's to directly address.
   b. Is one for which Ciena must integrate an updated third-party solution, or (where possible) update any dependency third-party tool distributed by Ciena.
   c. Requires an update to an external operating system (OS) operational environment (customer responsibility).
5. A recommendation or mitigation will be developed.
6. A product vulnerability advisory (PVA) will be issued.

Receipt and triage of vulnerability information for GA products

To safeguard consistent and exceptional customer support, Ciena will ensure a reliable companywide process for the collection and analysis of vulnerabilities that affect our products and services. The collection and triage of vulnerabilities enable not only consistent communication to our product development teams, but it also allows Ciena to have a consistent and transparent conversation with customers.

This portion of the process will cover how Ciena will evaluate vulnerabilities. It will establish rules for triage of the vulnerabilities and for assigning a Ciena severity level, as well as the roles of each participant in this step.

Ciena has established a global security team to facilitate the receipt, triage, and reporting of vulnerabilities associated with Ciena's networking systems, services, and software. Our team has collection and analysis processes for vulnerabilities intake and review from customers, industry leaders, and others. The vulnerability is then categorized in receipt and triaged for applicability and impact. Once determination is made on implications of the vulnerability, mitigation and remediation classifications are assigned.

To report an issue or vulnerability, please connect with Ciena through one of the following:

Email:

- PSIRT@ciena.com for product-specific vulnerability inquiries
- security@ciena.com for any concerns about Ciena or product issues

myCiena portal:

- Customers have direct and protected access to products support on the myCiena portal
- Contact the help desk
- Ciena monitors and reports as required on VINCE, the Vulnerability Information and Coordination Environment from Carnegie Mellon University's Software Engineering Institute
- Security researchers and external collaborators can reach Ciena using a publicly accessible and published security.txt file on our domain

In addition to the myCiena portal and VINCE, the following are approved methods by which Ciena will formally disseminate information to customers regarding vulnerabilities:

- Use Knowledge Base to reference product vulnerability notifications (PVNs), search common vulnerabilities and exposures (CVE) numbers, open a support ticket, and more
- CVE Program database

Process flow

Vulnerability and exposure management team: This team operates under the office of the Ciena chief information security officer (CISO). They receive regular vulnerability data feeds from multiple sources, which are curated with CVE and industry scoring information. Information received from this team should be considered reliable and actionable.

Supplier advisories: Our suppliers also advise Ciena regarding the products or services they provide to Ciena. When suppliers are brought into formal relationship with Ciena, it is recommended that the supplier be contractually obligated to forward vulnerability data they have to the vulnerability data ingest repository feed.

FOSS tracking: When Ciena uses free and open-source software (FOSS), all reasonable efforts should be made to subscribe to the associated advisory feed, or a manual process for regular updates should be put in place.

Product lifecycle validation tools: Ciena uses tools that identify product vulnerabilities throughout the product lifecycle. It is important to recognize these tools as trusted sources of vulnerability data. They should be identified and tracked in the Vulnerability data ingest repository.

Security researchers: A diverse community of security researchers conducts research on our products and could identify a vulnerability. These researchers may engage with Ciena through our security.txt public profile or bug bounty programs. Reports through this method will be acknowledged to the researchers within seven calendar days, and the reports will be forwarded to the Vulnerability data ingest repository.

Ciena product stakeholders: Internal product stakeholders may sometimes be made aware of a vulnerability. When that occurs, they must report their concern to their organization. Upon validation, an update to the Vulnerability data ingest repository should be made to ensure other teams that may have the same vulnerability are aware.

Determining Ciena's severity for a vulnerability

Vulnerabilities will typically be assigned a severity score by the cybersecurity community. The CVSS is currently the standard for community consensus scoring, and while this score is important to understand customer expectation and urgency, it does not set the impact for Ciena products. Each Ciena product team should conduct their own analysis, assessing the following factors:

1. Direct exposure

If the vulnerability is directly discoverable from an unauthenticated threat actor, it is considered directly exposed.

Customer and environmental mitigating factors should not be considered when determining direct exposure. As an example, customer-deployed firewalls or the use of a network operations center (NOC) do not remove this consideration. Assume the threat actor is in the same operational space and security domain when determining direct exposure.

2. Exploitable vulnerability

If there is a known exploit available for the vulnerability, the vulnerability is considered exploitable.

The longer a vulnerability exists on the product, the more likely an exploit will be created. The initial assessment occurs when first reported and should be reevaluated periodically.

3. Use in the wild

The existence of an exploit for a vulnerability, while important, must be considered in terms of real-world use. A theoretical or academic-level exploit does not require the same level of response as an exploit in use “in the wild” or in public space. The U.S. government Cybersecurity & Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog, the Exploit Database (exploit-db), and Bugtraq are valuable examples of sources for making this determination.

4. Authentication required

Does the vulnerability first require authenticated access for exploitation? A vulnerability that first requires user authentication should have its impact lowered.

5. Impact of exploitation

To determine impact, the product team should assume the vulnerability will be successful with maximum effectiveness. Once the vulnerability has been theoretically exploited, at a minimum, the following types of impact should be considered high:

- Data exposure: Customer data is exposed (any data that would not be publicly safe to disclose should be considered)
- Privilege escalation: Exploit that allows a user to gain a higher level of privilege within the product or service
- Denial of service (DoS): The exploit would bring down the product or service

Mitigation and remediation timelines

The number of days to mitigate or remediate is not inclusive of the time to determine the severity impact and score. It may take several days or weeks to determine the true impact. Our time to deliver a mitigation or remediation does not start until a determination of severity impact and scoring is complete.

The information set out herein is provided for general information purposes only and is subject to change at any time. Such information does not constitute legal or professional advice and is provided “as is” without warranty of fitness for a particular purpose or use, or any other kind, or compliance with applicable laws.