Vertiv Product Security

Overview

Vertiv Product Security is responsible for the security of products and services provided to Vertiv customers. For these areas, Product Security is responsible for vulnerability management and incident response, security requirements, and security testing.

Our People

The Vice President, Information and Product Security, who reports to the Chief Information Officer, leads the Information Security department. This position oversees all aspects of cyber risk management, IT compliance, and data privacy. Organizational, physical, and operational security is maintained by a full-time staff of professionals with defined roles and responsibilities in various information security specialties.

The Director of Product Security reports to the Vice President, Information and Product Security and oversees all activities. Product Security works closely with engineering and development teams to review and evaluate the security of Vertiv products. To facilitate this, Product Security is organized into four pillars: Architecture, Development, Testing, and Governance.

The Architecture pillar is responsible for performing design reviews of products against Vertiv security standards. They also lead the security aspects for new technology evaluations.

The Development pillar works closely with engineering teams to assist with various security-related aspects of the DevSecOps process. This includes code signing, code review, and integrating security scans into coding processes.

The Testing pillar is responsible for all testing aspects of security including penetration testing of new products. This involves automated scanning using various tools and manual attacking to identify weaknesses that others might be able to exploit.

The Governance pillar is responsible for managing the vulnerability and incident response process, understanding industry trends, and keeping Vertiv's security-related requirements up to date with those trends and new security frameworks or standards, as well as ensuring documentation related to these processes are updated as needed.

Our Processes

Product Security is integrated into Vertiv's overall New Product Development and Introduction (NPDI) process to ensure all new products are developed with security in mind. All new products are expected to meet Vertiv's SECURE requirements. These requirements have been derived from multiple industry security certifications as well as industry best practices. At different phases of new product development, security related risks are evaluated against Vertiv's SECURE requirements, and changes are suggested or mandated depending on the level of risk. This process includes static and dynamic testing of code and binaries.

Product Security is also responsible for overseeing the Vulnerability Management and Incident Response Process for vulnerabilities related to Vertiv products and services. Vulnerabilities can be reported to Product Security through our Security Support Center page at **https://www.vertiv.com/en-us/support/security-support-center/**.

Responsible Disclosure

We encourage coordinated disclosure of product security vulnerabilities. Security reasearchers, industry groups, government organizations and vendors can report potential product security vulnerabilities to Vertiv.

Report a Product Security Concern

If the vulnerability affects **only a Vertiv product**, please click "Report a Product Security Concern" below.

Please include the following:

- Product and version
- Description of the potential vulnerability
- Any special configuration required to reproduce the issue
- Proof of concept or exploit code, if available
- Potential impact
- CVE #
- Company or Organization
- Tool used to uncover potential vulnerability

REPORT A PRODUCT SECURITY CONCERN

Report other Security Concerns

For all security issues, please click "Report other Security Cocerns" below:

Please include the following:

- Website URL or location
- Type of potential vulnerability (XSS, Injection, etc.)
- Instructions to reproduce the potential vulnerability
- Proof of concept or exploit code, including how an attacker could exploit the potential vulnerability
- Potential impact

REPORT OTHER SECURITY CONCERNS

We take security concerns seriously and work to evaluate and address them in a timely manner. Response timelines will depend on many factors, including: the severity, the product affected, the current development cycle, QA cycles, and whether the issue can only be updated in a major release.

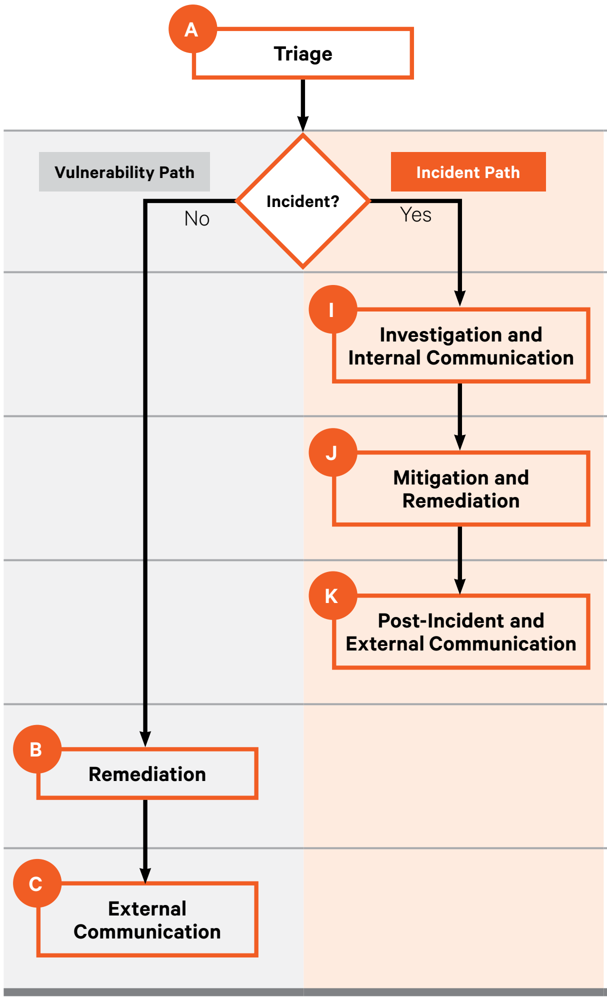
Remedation may take one or more of the following forms:

- A new release
- A patch
- Instructions to download and install an update or patch from a third-party
- A workaround to mitigate the vulnerability

Notwithstanding the foregoing, not all reported concerns will result in validated vulnerabilities, and we cannot guarantee that reported concerns will result in specific resolutions, corrections, or mitigating actions for such concerns.

This process includes a simple intake process for external concerns about product security, robust monitoring of software components utilized in product development, quick understanding of scope and risk with discovered vulnerabilities, immediate connection to the right leaders for swift action, and consistent process for all items.

The image below shows a high-level overview of the process. SLAs have been established with engineering teams in line with industry best practices.



What	Responsible	Notified
A Triage	Core Product Security Vulnerability Management Team	N/A
Incident?	Core Product Security Vulnerability Management Team	N/A
I Investigation and Internal Communication	Core Product Security Incident Response Team	Extended Product Security Incident Response Team
J Mitigation and Remediation	Core Product Security Incident Response Team	Extended Product Security Incident Response Team
K Post-Incident and External Communication	Core Product Security Incident Response Team	Extended Product Security Incident Response Team
B Remediation	Core Product Security Vulnerability Management Team	Extended Product Security Vulnerability Management Team
C External Communication	Core Product Security Vulnerability Management Team	Extended Product Security Vulnerability Management Team

© 2022 Vertiv Group Corp. All rights reserved. Vertiv™ and the Vertiv logo are trademarks or registered trademarks of Vertiv Group Corp. All other names and logos referred to are trade names, trademarks or registered trademarks of their respective owners. While every precaution has been taken to ensure accuracy and completeness here, Vertiv Group Corp. assumes no responsibility, and disclaims all liability, for damages resulting from use of this information or for any errors or omissions. Specifications, rebates and other promotional offers are subject to change at Vertiv's sole discretion upon notice.