The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that manages the receipt, investigation, and public reporting of security vulnerability information that is related to Cisco products and networks.

**Incident Handling Process**

1. **PSIRT is notified of a security incident**
2. PSIRT prioritizes and identifies resources
3. PSIRT coordinates product impact assessment and fixes
4. Customers and the public are notified simultaneously

**COMPLETE PROTECTION:**

PSIRT investigates vulnerabilities across the entire Cisco product portfolio.
Benefits

Industry Standards: Follows standard rules, policies, and scoring systems

Consistency: Applies the same mature process across the Cisco portfolio, even as the product line grows

Best-in-Class Service: Provides dedicated support for product security and network protection

Speed: Quickly assigns CVEs for security vulnerabilities

Collaboration: Works with product teams across Cisco and third parties

Transparency: Publicly discloses both internally and externally reported vulnerabilities

Policy

PSIRT investigates all reports, regardless of the Cisco software code version, through the last day of support for a given product.

Issues will be prioritized based on the potential severity of the vulnerability and other environmental factors. Ultimately, the resolution of a reported incident may require upgrades to products that are under active support from Cisco. Review the Cisco Security Vulnerability Policy to learn about:

+ How to report or obtain support for a suspected security vulnerability
+ Details on the incident response process
+ Communications and disclosure plans

Receiving Security Vulnerability Information from Cisco

There are several ways to stay connected and receive the latest security vulnerability information from Cisco.

Cisco Security: cisco.com/security
Contact PSIRT: psirt@cisco.com
RSS feeds: http://tools.cisco.com/security/center/rss.x?i=44
Cisco PSIRT openVuln API: https://developer.cisco.com/site/PSIRT/