Cisco Product Security Incident Response Team

Protection. Security. Transparency.



The Cisco Product Security Incident Response Team (PSIRT) is a dedicated, global team that receives, investigates, and publicly discloses security vulnerability information. PSIRT also manages forensic investigations and escalations that affect Cisco products and services.

Vulnerability Management and Disclosure Process

- PSIRT is notified of a security incident
- PSIRT prioritizes incidents and identifies resources
- PSIRT coordinates product impact assessment and fixes
- PSIRT notifies customers and the public simultaneously

Incident Response Process

- Customers notify PSIRT of a possible security incident
- PSIRT requests and analyzes forensic data
- PSIRT determines if a vulnerability exists and assesses the impact
- PSIRT advises customers on a resolution plan

- More than 30 years of experience alerting customers about vulnerabilities in Cisco products
- The only group within Cisco that is authorized to disclose vulnerability information to customers
- Global team of incident managers, risk managers, and content managers that provides customer support
- ISO 29147 compliant

[Cisco proprietary code] + [Third-party software components]

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

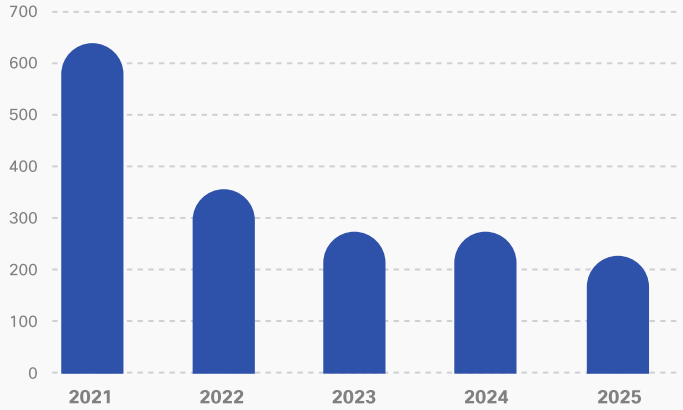
Best-in-Class Service: Provides dedicated support for product security and network protection

Speed: Rapidly assigns CVE IDs and identifies mitigations

Transparency: Publicly discloses both internally and externally reported vulnerabilities

Customer Security Focus: Protects customer information, infrastructure, and brand reputation

Cisco CVE Assignments



PSIRT assigns Common Vulnerabilities and Exposure (CVE) identifiers to internally and externally found vulnerabilities across hundreds of products, which reflects Cisco's commitments to transparency and helping customers mitigate risk.

Policy

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

PSIRT prioritizes issues based on the potential severity of the vulnerability and other environmental factors. Ultimately, resolving 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
- The incident response process
- Communications and disclosure plans

Access Cisco Security Vulnerability Information

There are several ways to stay connected and access the latest Cisco security vulnerability information:

Cisco Security: cisco.com/security
Contact PSIRT: psirt@cisco.com
RSS feeds: http://tools.cisco.com/security/centers/rss.x?i=44
My Notifications: https://www.cisco.com/c/en/us/support/web/tools/cns/notifications.html
Cisco PSIRT openVuln API: https://developer.cisco.com/site/PSIRT/

© 2026 Cisco and/or its affiliates. All rights reserved.