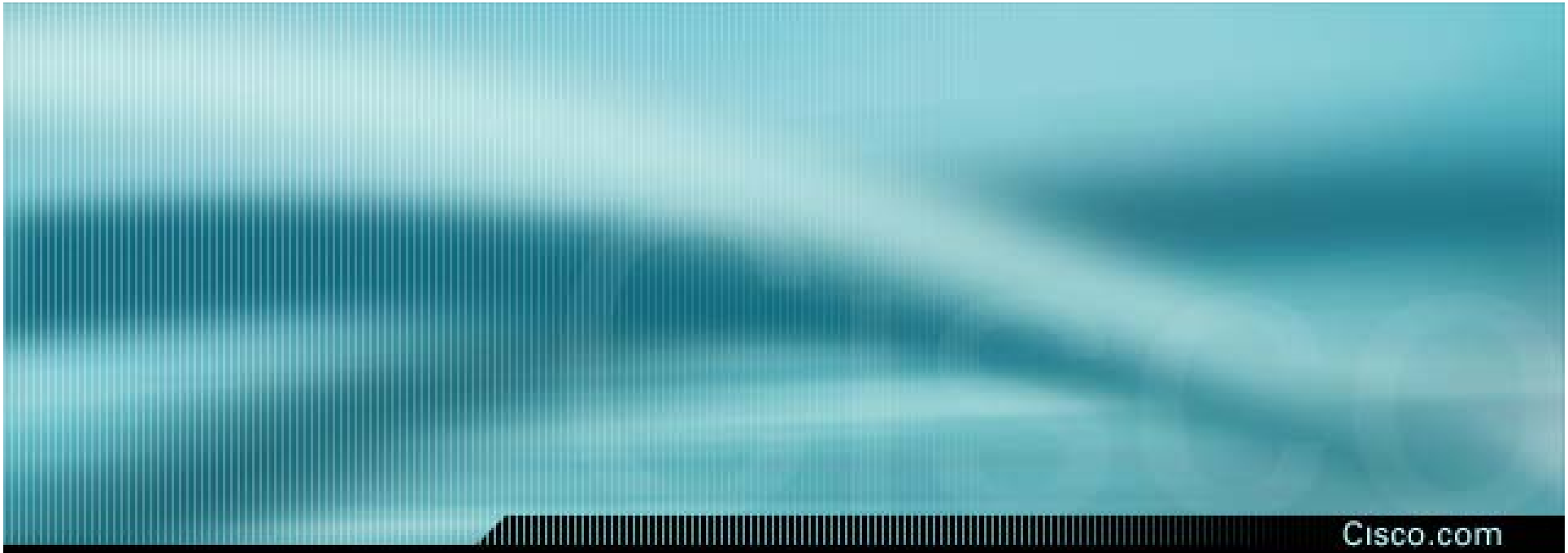

Cisco Systems



Cisco PSIRT

Dario Ciccarone

Incident Manager, Product Security Incident Response Team

<dciccaro@cisco.com>

What Is PSIRT?

- **Cisco's Product Security Incident Response Team**
- **PSIRT's Mission:**

  Help customers improve their network security through the resolution and prevention of security vulnerabilities in Cisco products, provide specialized support to handle customer security incidents, and represent Cisco in the incident response and product security communities.

The Team

- Reachable via psirt@cisco.com
- 12 global Incident Managers (IM) who are available 24x7
- In addition, multiple corporate liaisons, including Public Relations, Legal

About PSIRT

Cisco.com

- PSIRT covers all Cisco products
- Creates and publishes Cisco Security Advisories and Notices
- Handles customer security incidents (e.g. active intrusions, Denial of Service attacks)
- Assists with computer and network forensics: analysis, packet traces, logs, second opinions
- Our service is free of charge

About PSIRT (Cont.)

- Member of FIRST (Forum of Incident Response Teams)
- One of the several Cisco teams focused on security issues (others include Infosec, Security Consulting, CIAG)
- Is the point of contact for receiving and pursuing external reports of vulnerabilities in Cisco products. Includes liaison with multiple internal and external organizations, as well as law enforcement

Functions Not Performed By PSIRT

These are normally provided by Cisco's Technical Assistance Center (TAC) or a customer's usual support channel:

- **Proactive setup or general configuration questions**
- **Security policy or design issues**
- **Ordinary (non-security) defects with Cisco products**
- **Lost enable passwords**

Who Qualifies for PSIRT's Assistance?

Cisco.com

- Cisco products are likely to be involved – but this is not a requirement
- A maintenance contract is not necessary
- PSIRT should be contacted if a customer specifically asks for our involvement, if the TAC engineer feels that this is a new or unknown attack, or if the caller is identified as a law enforcement officer or member of an external incident response team

When Does PSIRT Disengage From a Case?

Cisco.com

- When the customer asks for an extensive analysis – referred to the SPA team
- When customer asks for design help – referred to Consulting or pre-sales support
- Forensic analysis done only to the extent which determines the vulnerability of our products – but not for eventual prosecution
- When it is established that none of our products are involved

Interaction With Other Vendors

- If we discover a vulnerability in a third-party product we will report it to the vendor
- If we discover a vulnerability in a competitor's product, we will report it to the vendor or a neutral third party (e.g. CERT/CC)

PSIRT Interaction Within Cisco

Cisco.com

Interaction With External Organizations

Cisco.com

- USA: NIPC, FBI, IT-ISAC
- UK: ICF, NHTCU
- Europe: TF-CSIRT
- Global: FIRST

PSIRT Modus Operandi

- Confidentiality
- Sharing information on a need-to-know basis
- Separate case tracking system
- Offices with solid walls

PSIRT's Customer-Facing Deliverables

Cisco.com

- **Security Advisories**
- **Other responses**
  - **Security Notices**
  - **Technical Tips**
  - **Product Bulletins**
  - **Follow-up to a mailing list (e.g. BugTraq)**

Security Advisory: Key Points

Cisco.com

- A severe security issue that represents a potential vulnerability
- Typically entitles Cisco customer to no-cost fixed software

Other Responses

- Less severe security issues (e.g. third party patches, CDP)
- Typically does not entitle a customer to no-cost upgrades
- Generally not time critical

What Constitutes a Security Issue?

- A breach of confidentiality, integrity, or availability
- Could be one or more of the above

Some Metrics For Security Issue Evaluation

- Is it actually broken?
- Is it a remote or local vulnerability?
- Is it publicly known? Has it been exploited?
- How easy is to exploit it? What protocol is used? Are there existing scripts with which to perform the exploitation?

Triggers For Releasing an Advisory

Cisco.com

- It is widely exploited
- The software is fixed and available to customers

Advisory Release Procedure

Cisco.com

- Normally, on Tuesdays and Wednesdays
- In emergency – at any time
- All customers receive notice at the same time
- The Advisory is sent to the mailing list

  cust-security-announce@cisco.com

PSIRT's Proactive Role

- Evaluating new and existing products
- Advising Cisco's Technology Groups (TG) on the development of new features
- Providing additional expertise for the TGs
- Pushing for new features
- Driving improvements in code testing across Cisco

Working Together At Cisco

- We share focus on product security with multiple groups
  - STAT
  - Consulting Engineering
- We rely on other teams for notification and research of new vulnerabilities
  - TAC
  - Advanced Services
  - External sources

Contact Details

- psirt@cisco.com for non-emergency
- security-alert@cisco.com for emergencies
- +1 877 228 7302 (toll-free in North America)
  +1 408 525 6532 (elsewhere in the world)
- Contact TAC and ask for PSIRT
- www.cisco.com/go/psirt