# Cisco Product Security Incident Response

## Product Security Incident Response Team

<psirt@cisco.com>


© 1999, Cisco Systems, Inc.

**Product Security Incident Managers:**

**Jim Duncan**

**<jnduncan@cisco.com>**

**Lisa Napier**

**<lnapier@cisco.com>**

**Damir Rajnovic**

**<drajnovi@cisco.com>**

PSIRT Evangelist:

Richard Aceves

Serviceability Design

<raceves@cisco.com>

# About PSIRT

- **The PSIRT covers ALL Cisco products! (Not just security products)**
- **Handle customer's security incidents**
- **Our service is free of charge**
- **Liaison member of FIRST (Infosec is the full member)**
- **One of the several groups which deals with security (some of the others are: Infosec, SecurityConsulting, SNS, Consulting)**


© 1999, Cisco Systems, Inc.

# Product Security Incident Manager

- **Incident Manager is a member of the Escalation Team**
- **Responds to active attacks; mostly intrusions or denial-of-service (DoS) attacks**
- **Assists with computer and network forensics: analysis, packet traces, logs, second opinions**
- **Point-of-Contact for receiving and pursuing external reports of vulnerabilities in Cisco products**
- **Proactive work on new products and evaluation of existing ones**


© 1999, Cisco Systems, Inc.

# External Liaisons

- **PSIRT members are active in US and EU area:**
  - **FBI (EU)**
  - **National Infrastructure Protection Center (US)**
  - **Internet Crime Forum (UK)**
  - **National Criminal Intelligence Service (UK)**
  - **G8 Hi-Tech Crime Subcommittee**
  - **Partnership for Critical Infrastructure Security (US)**


© 1999, Cisco Systems, Inc.

# Who Qualifies for PSIRT Help?

- **Cisco products likely to be involved, but not required**
- **No maintenance contract required**
- **Case will be send to PSIRT if customer specifically asks**
- **The same if caller is identified as law enforcement officer or member of an incident response team**
- **Otherwise the normal queue process applies**


© 1999, Cisco Systems, Inc.

# Don’t Send This Stuff to PSIRT

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


© 1999, Cisco Systems, Inc.

# Confidentiality

- **Confidentiality is even more important for security incidents than ordinary cases**
- **Information leaks can hurt the customer and Cisco**
- **Minimize discussion to maintain confidentiality**


© 1999, Cisco Systems, Inc.

# Confidentiality (cont.)

- **PSIRT uses its own tracking system which is separate from the rest of the company**
- **Only PSIRT members do have access to it**
- **Mailing list is closed with strictly controlled members**
- **Strict application of need-to-know rules for every information and issue which we are handling**


© 1999, Cisco Systems, Inc.

# Contacting PSIRT

- **<psirt@cisco.com> for non-emergency messages**
  **<security-alert@cisco.com> for emergencies**
- **+1 877 228 7302 (toll-free in North America)**
  **+1 408 525 6532 (elsewhere in the world)**
- **If no response, contact Incident Managers separately**
  **http://www-tac.cisco.com/Teams/PSIRT/psirt-members.html**
- **Fallback provided by PSIRT liaison members, Escalation Teams, and the TAC Manager on Duty**


© 1999, Cisco Systems, Inc.

# References

- **PSIRT web page**
  **http://www.cisco.com/warp/public/707/sec_incident_response.shtml**
- **Security Advisories and guides on CCO**
  **http://www.cisco.com/warp/public/707/advisory.html**


© 1999, Cisco Systems, Inc.