

Control System Software Vulnerability Coordination and Disclosure

**Art Manion
CERT Coordination Center
March 6, 2007**

Vulnerability Definition

- ◆ **A set of conditions that allows the violation of an explicit or implicit security policy**
- ◆ **The violation has an impact (first order) or consequence**
- ◆ **Often a *software* defect (implementation flaw), can also be a design or configuration error (or choice), unexpected interaction between systems, or changing environment**

CERT/CC Vulnerability Remediation

- ◆ **Mission: Reduce the number of, and risk posed by software vulnerabilities**
- ◆ **Methodology**
 - Collect: Monitor public sources, accept private reports
 - Analyze: Understand mitigations and technical threat
 - Coordinate: Notify vendors and other stakeholders
 - Publish: Provide actionable remediation advice

Questions About Vulnerabilities

- ◆ **Do you create or use software with vulnerabilities?**
- ◆ **How do you find out about vulnerabilities?**
- ◆ **Do you have sufficient information about vulnerabilities to make an accurate risk decision?**
- ◆ **What are appropriate responses to vulnerabilities?**

Questions About Vulnerabilities

- ◆ **Do you create or use software with vulnerabilities?**
- ◆ How do you find out about vulnerabilities?
- ◆ Do you have sufficient information about vulnerabilities to make an accurate risk decision?
- ◆ What are appropriate responses to vulnerabilities?

Questions About Vulnerabilities

- ◆ Do you create or use software with vulnerabilities?
- ◆ **How do you find out about vulnerabilities?**
- ◆ Do you have sufficient information about vulnerabilities to make an accurate risk decision?
- ◆ What are appropriate responses to vulnerabilities?

Questions About Vulnerabilities

- ◆ Do you create or use software with vulnerabilities?
- ◆ How do you find out about vulnerabilities?
- ◆ **Do you have sufficient information about vulnerabilities to make an accurate risk decision?**
- ◆ What are appropriate responses to vulnerabilities?

Questions About Vulnerabilities

- ◆ Do you create or use software with vulnerabilities?
- ◆ How do you find out about vulnerabilities?
- ◆ Do you have sufficient information about vulnerabilities to make an accurate risk decision?
- ◆ **What are appropriate responses to vulnerabilities?**

Questions About Vulnerabilities

- ◆ Do you create or use software with vulnerabilities?
- ◆ How do you find out about vulnerabilities?
- ◆ **Do you have sufficient information about vulnerabilities to make an accurate risk decision?**
- ◆ What are appropriate responses to vulnerabilities?

Vulnerability Disclosure

- ◆ **Coordination and publication provide information about vulnerabilities—this is disclosure. Without disclosure, there is no resolution.**
 - Who needs to know?
 - Why do they need to know?
 - What information about the vulnerability, what level of detail?
 - How is the information conveyed?
 - When during the disclosure process?

Vulnerability Disclosure

- ◆ **Coordination and publication provide information about vulnerabilities—this is disclosure. **Without disclosure, there is no resolution.****
- Who needs to know?
- Why do they need to know?
- What information about the vulnerability, what level of detail?
- How is the information conveyed?
- When during the disclosure process?

CERT/CC Approach

◆ Apply existing methodology

- PCSF 2006
 - Five reports, one Vulnerability Note, one vendor contact
- PCSF 2007
 - 33 reports, 5 Vulnerability Notes, 22 vendor contacts

◆ Elicit comments on disclosure process

◆ Develop means to disclose information about control system vulnerabilities safely and effectively

CERT/CC Approach

◆ Apply existing methodology

- PCSF 2006
 - Five reports, one Vulnerability Note, one vendor contact
- PCSF 2007
 - 33 reports, 5 Vulnerability Notes, 22 vendor contacts

◆ Elicit comments on disclosure process

◆ Develop means to disclose information about control system vulnerabilities safely and effectively