



Vulnerability Disclosure

Art Manion
Process Control Systems Industry Conference

August 2008



Software Engineering Institute | Carnegie Mellon

© 2008 Carnegie Mellon University

Disclosure is Coordination

Process

- **Collect:** Monitor public sources, accept private reports, perform original research
- **Analyze:** Understand vulnerability, attack vectors, mitigations, threats, context
- **Coordinate:** Vendors, critical infrastructure, researchers, trusted experts, CSIRTs, other stakeholders
- **Disclose:** Document vulnerability, provide actionable remediation information

Goals

- Balance multiple competing objectives
- Minimize (potential) damage

Collaboration

- Work closely with DHS/US-CERT, vendors, researchers, CSIRTs

Coordination is Disclosure

“Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman.”

– Louis Brandeis

Disclosure combats information asymmetry

Without accurate vulnerability information, customers cannot make informed decisions

- Market for Lemons (Akerlof)

Reporting, coordination, and publication provide information about vulnerabilities—this is disclosure. *Without disclosure, there can be no resolution.*

Control Systems Vulnerability Notes



US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

[Vulnerability Notes Database](#)

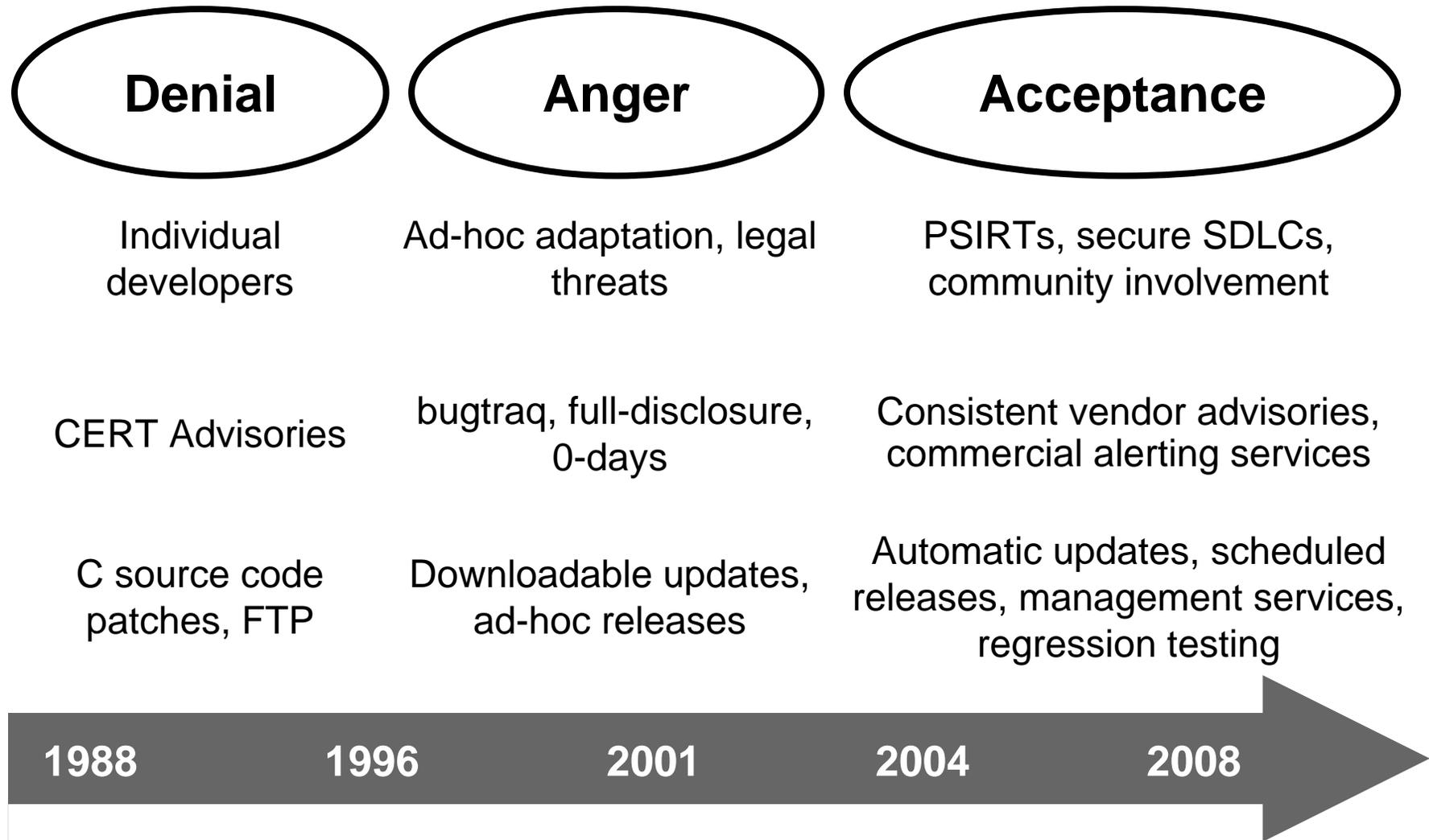
[Search Vulnerability Notes](#)

[Vulnerability Notes Help Information](#)

Search Results

	Date Published	ID	Name
View Notes By Name	06/11/2008 12:55:41 PM	VU#476345	Citect CitectSCADA buffer overflow
ID Number	05/06/2008 04:01:06 PM	VU#596268	Wonderware SuiteLink null pointer dereference
CVE Name	01/25/2008 03:32:45 PM	VU#339345	GE Fanuc Proficy Information Portal allows arbitrary file upload and execution
Date Public	01/25/2008 03:30:28 PM	VU#308556	GE Fanuc CIMPLICITY HMI heap buffer overflow
Date Published	01/25/2008 03:26:36 PM	VU#180876	GE Fanuc Proficy Information Portal transmits authentication credentials in plain text
Date Updated	12/14/2007 08:19:53 AM	VU#205073	Gesytec Easyon OPC Server fails to properly validate OPC server handles
Severity Metric	11/19/2007 10:38:25 AM	VU#138633	Invensys Wonderware InTouch creates insecure NetDDE share
	05/03/2007 04:18:34 PM	VU#213516	LiveData Protocol Server fails to properly handle requests for WSDL files
	05/02/2007 02:35:37 PM	VU#711420	LiveData Server fails to properly handle Connection-Oriented Transport Protocol packets
	03/22/2007 12:34:45 PM	VU#296593	NETxAutomation NETxEIB OPC Server fails to properly validate OPC server handles
	03/19/2007 11:43:03 AM	VU#926551	Takebishi Electric DeviceXPlorer OPC Server fails to properly validate OPC server handles
	01/17/2007 10:43:42 AM	VU#145825	SISCO OSI stack fails to properly handle malformed packets
	01/02/2007 12:43:20 PM	VU#251969	ICONICS Dialog Wrapper Module ActiveX control vulnerable to buffer overflow
	09/20/2006 03:15:49 PM	VU#468798	SISCO OSI stack fails to properly validate packets
	07/27/2006 02:19:39 PM	VU#372878	Tamarack MMSd components fail to properly handle malformed packets
	05/16/2006 03:45:03 PM	VU#190617	LiveData ICCP Server heap buffer overflow vulnerability

IT Vulnerability Response Evolution



Questions

Vulnerability questions:

- Do you create or use software with vulnerabilities?
- How do you find out about vulnerabilities?
- Do you have sufficient information about vulnerabilities to make accurate risk assessments and response?

Disclosure questions:

- Who needs to know?
- Why do they need to know?
- What type/level of information?
- How is the information conveyed?
- When during the disclosure process?
- How will information benefit adversaries?