Demystifying Disclosure
How and Why to Get Started

Art Manion
CERT Coordination Center
CyberMedRx
2015-12-04
Coordinated Vulnerability Disclosure

Vulnerability
• Set of conditions that violates security expectations, often implementation defects (bugs)

Disclosure
• Initial communication of vulnerability information

Coordination
• Communication and other disclosure activity, often conducted privately before public disclosure
CERT/CC Disclosure 1988

CA-88:01

CERT Advisory
December 1988
ftpd vulnerability

** The sendmail portion of this advisory is superseded by CA-95:05. **

There have been several problems or attacks which have occurred in the past few weeks. In order to help secure your systems we have gathered the following suggestions:

1) Check that you are using version 5.59 of sendmail with the debug option DISABLED. To verify the version try the following commands. Use the telnet program to connect to your mail server. Telnet to your hostname or localhost with 25 following the host. The sendmail program will print a banner which will have the version number in it. You need to be running version 5.59. Version 5.61 will be released on Monday 12/12/1988. Any version less than 5.59 is a security problem.
Vulnerability Notes Database
Advisory and mitigation information about software vulnerabilities

Vulnerability Note VU#870761
Dell Foundation Services installs root certificate and private key (eDellRoot)

Original Release date: 24 Nov 2015 | Last revised: 01 Dec 2015

Overview
Dell Foundation Services installs the eDellRoot certificate into the Trusted Root Certificate Store on Microsoft Windows systems. The certificate includes the private key. This allows attackers to create trusted certificates and perform impersonation, man-in-the-middle (MiTM), and passive decryption attacks, resulting in the exposure of sensitive information.
## Why Start?

<table>
<thead>
<tr>
<th>Minimize harm</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Protect patient safety, privacy</td>
<td>• Theft of health care data</td>
</tr>
<tr>
<td>• Costs to all stakeholders</td>
<td>• Intentional harm</td>
</tr>
<tr>
<td></td>
<td>• Accidental or incidental harm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Business drivers</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Self regulation</td>
<td>• Vulnerabilities exist</td>
</tr>
<tr>
<td>• Manage disclosure events</td>
<td>• Security research finds vulnerabilities</td>
</tr>
<tr>
<td>• Focus external research efforts</td>
<td>• Vendors, providers, supply chain, SOUP, OTS</td>
</tr>
<tr>
<td>• Market differentiation</td>
<td></td>
</tr>
</tbody>
</table>
Why Start?

Minimize harm

• Protect patient safety, privacy
Myths

Researchers are out for fame and fortune
• Maybe so
• Many want to protect users
• Misunderstanding
Public disclosure increases risk
• It might
• Attackers know, but vendors and users don’t
Public disclosure looks bad
• All software and systems have vulnerabilities
• Publishing fixes and mitigation advice demonstrates responsibility
Security updates require 510(k) recertification
• Possible, but unlikely
  • “The FDA typically does not need to review or approve medical device software changes made solely to strengthen cybersecurity.”
EHR Vulnerabilities

Joshua Mandel
http://smarthealthit.org/2014/04/ehr-security-vulnerability-reporting/

HL7 C-CDA XML vulnerabilities

- JavaScript/HTML injection

Successfully contacted one vendor

- Reported over weekend to known contact
- Fixed in five days

Tried to reach 82 other vendors

- Manual web site review
- security@ and other email addresses
- Web forms
- <10% response rate
How to Get Started

Current and previous experience
• Disclosure policy and practices
• Experience of other sectors

Small steps
• Change takes time

External support
• I Am The Cavalry, NH-ISAC, CERT/CC, ICS-CERT, FDA, NCCoE, MDISS

Commercial options
• Vulnerability management, bug bounty, and security research services and platforms
International Standards

ISO/IEC JTC 1/SC 27 Security techniques
• WG 3 Security evaluation, testing and specification
29147 Vulnerability disclosure
• Receive and respond to vulnerability reports
• Publish advisory and remediation information
30111 Vulnerability handling
• Internal processes to investigate, develop remediation, improve SDL

Published in 2013/2014, 138/58 CHF
• Under revision, expect to be available early 2017
• For free if possible
## HackerOne Vulnerability Coordination Maturity Model

<table>
<thead>
<tr>
<th>Capability</th>
<th>Basic (Crawl)</th>
<th>Advanced (Walk)</th>
<th>Expert (Run)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational</td>
<td>Executive Support</td>
<td>Policy &amp; Process</td>
<td>Dedicated Personnel</td>
</tr>
<tr>
<td>Engineering</td>
<td>Tracking &amp; Processing</td>
<td>Track, Triage &amp; Fix</td>
<td>SDL Feedback</td>
</tr>
<tr>
<td>Communications</td>
<td>Issue Advisories</td>
<td>Internal &amp; External</td>
<td>Information Sharing</td>
</tr>
<tr>
<td>Analytics</td>
<td>Process Raw Data</td>
<td>Root Cause Analysis</td>
<td>Real-time Tracking</td>
</tr>
<tr>
<td>Incentives</td>
<td>Thanks &amp; Swag</td>
<td>Bounty Awards</td>
<td>Market Impact</td>
</tr>
</tbody>
</table>

Adapted from [https://hackerone.com/blog/vulnerability-coordination-maturity-model]
Faster: Industrial Control Systems

Vulnerability Note VU#468798: SISCO OSI stack fails to properly validate packets
  • 2005-02-25
First ICS-CERT Advisory: ICSA-10-070-02: Rockwell PLC5/SLC5/0x/RSLogix Security Vulnerability
  • 2010-03-10
Five years between first public disclosure and sector-specific coordinator
References

http://www.fda.gov/RegulatoryInformation/Guidances/ucm077812.htm
http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm
https://hackerone.com/blog/vulnerability-coordination-maturity-model
https://lost-contact.mit.edu/afs/cern.ch/project/security/ciac/secdocs/cert/88-01.txt-ftpd.hole
http://www.kb.cert.org/vuls/id/870761
http://www.kb.cert.org/vuls/id/468798
https://ics-cert.us-cert.gov/advisories/ICSA-10-070-02
http://smarthealthit.org/2014/04/ehr-security-vulnerability-reporting/