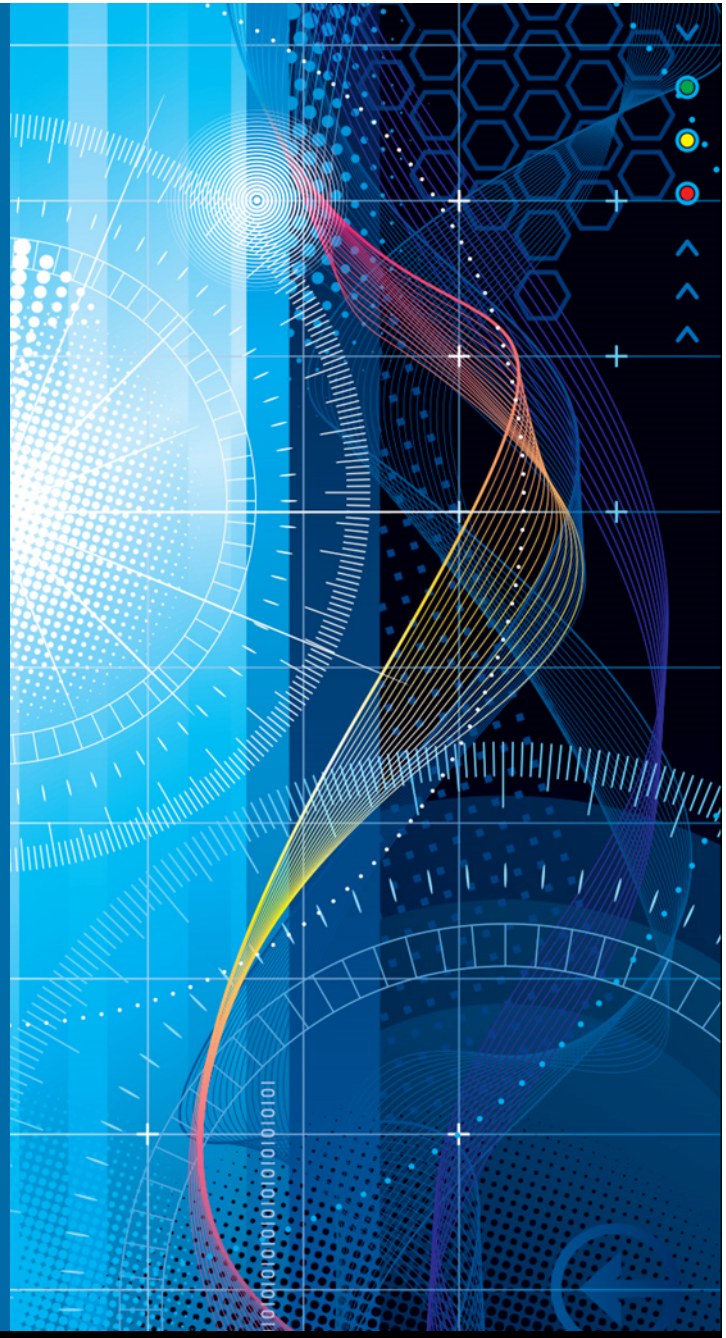
Demystifying Disclosure
How and Why to Get Started

Art Manion

CERT Coordination Center

CyberMedRx

2015-12-04



© 2015 Carnegie Mellon University

This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of Department of Homeland Security or the United States Department of Defense.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon®, CERT® and CERT Coordination Center® are registered marks of Carnegie Mellon University.

DM-0003157

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

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT/CC Disclosure 1988

CA-88:01

CERT Advisory
December 1988
ftpd vulnerability

- ----------

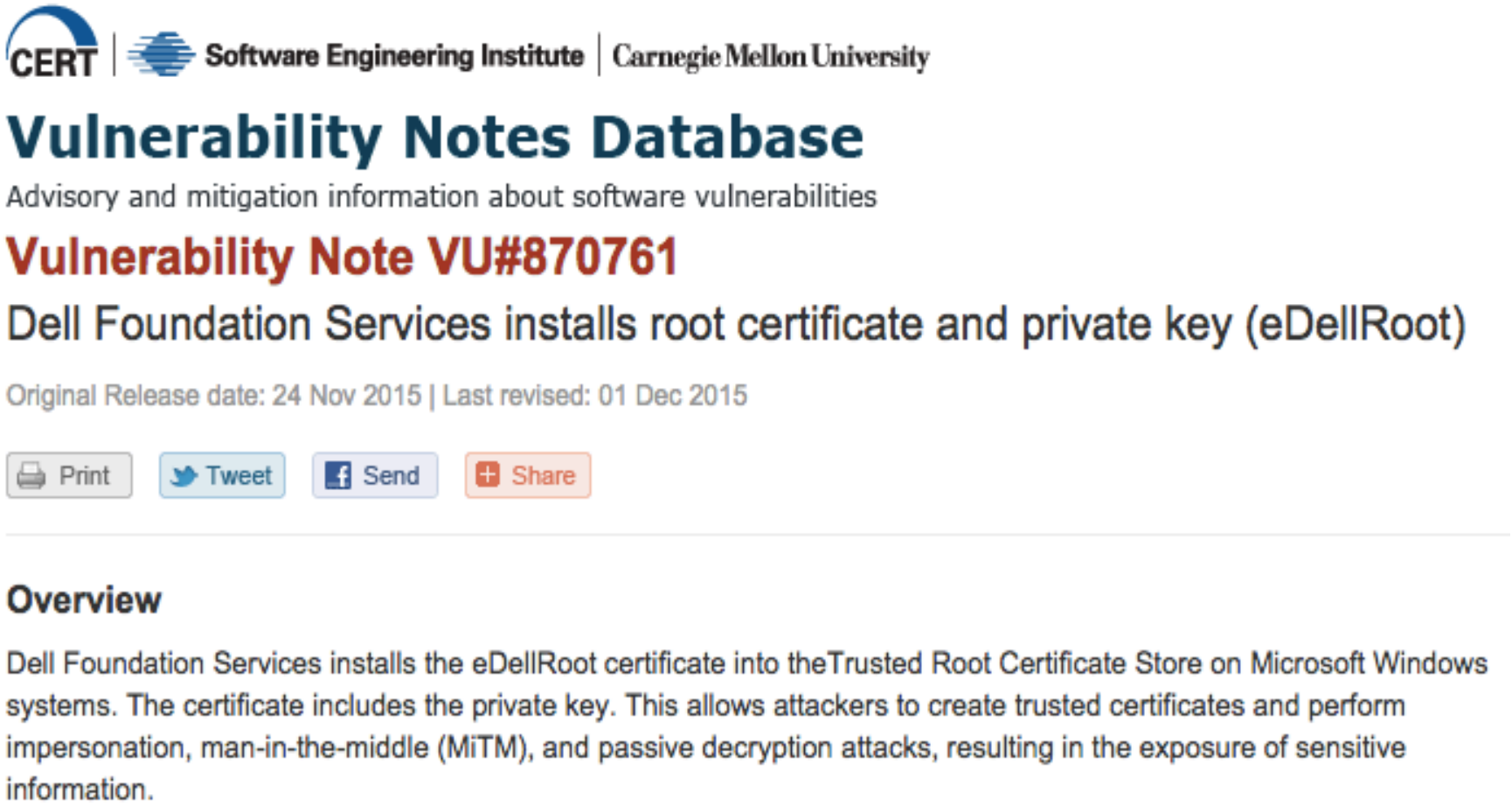
** The sendmail portion of this advisory is superseded by CA-95:05. **

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.

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

CERT/CC Disclosure 2015



CERT | Software Engineering Institute | Carnegie Mellon University

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

Print Tweet Send Share

Overview

Dell Foundation Services installs the eDellRoot certificate into theTrusted 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.

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Why Start?

Minimize harm
- Protect patient safety, privacy
- Costs to all stakeholders

Threat
- Theft of health care data
- Intentional harm
- Accidental or incidental harm

Business drivers
- Self regulation
- Manage disclosure events
- Focus external research efforts
- Market differentiation

Responsibility
- Vulnerabilities exist
- Security research finds vulnerabilities
- Vendors, providers, supply chain, SOUP, OTS

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

Why Start?

Minimize harm

- Protect patient safety, privacy

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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.*"

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

HackerOne Vulnerability Coordination Maturity Model

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

Adapted from <https://hackerone.com/blog/vulnerability-coordination-maturity-model>

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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

© 2015 Carnegie Mellon University
This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

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/security-vulnerabilities-in-ccda-display/

http://smarthealthit.org/2014/04/case-study-security-vulnerabilities-in-ccda/

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

© 2015 Carnegie Mellon University

This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.