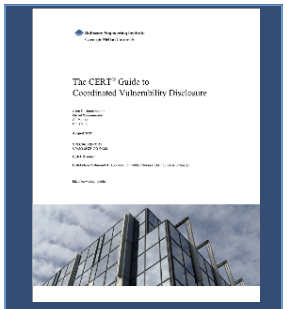
The CERT Guide to Coordinated Vulnerability Disclosure

This is the web edition of *The CERT® Guide to Coordinated Vulnerability Disclosure*. We've reproduced the original report here in its entirety to make it easier to find the topic you're looking for. We're also in the process of revising the guide based on feedback we've received since its original publication. Got a suggestion? Submit it here.

Authors:

Allen D. Householder
Garret Wassermann
Art Manion
Chris King

Originally Published as CMU/SEI-2017-SR-022



Download the Original PDF version

CERT/CC Blog post announcing the publication of the Guide

Abstract

Security vulnerabilities remain a problem for vendors and deployers of software-based systems alike. Vendors play a key role by providing fixes for vulnerabilities, but they have no monopoly on the ability to discover vulnerabilities in their products and services. Knowledge of those vulnerabilities can increase adversarial advantage if deployers are left without recourse to remediate the risks they pose. Coordinated Vulnerability Disclosure (CVD) is the process of gathering information from vulnerability finders, coordinating the sharing of that information between relevant stakeholders, and disclosing the existence of software vulnerabilities and their mitigations to various stakeholders including the public. The CERT Coordination Center has been coordinating the disclosure of software vulnerabilities since its inception in 1988. This document is intended to serve as a guide to those who want to initiate, develop, or improve their own CVD capability. In it, the reader will find an overview of key principles underlying the CVD process, a survey of CVD stakeholders and their roles, and a description of CVD process phases, as well as advice concerning operational considerations and problems that may arise in the provision of CVD and related services.

CVD Quick Start

When we finished the first version of The CERT Guide to Coordinated Vulnerability Disclosure, we noticed folks kept commenting on its length. Feedback we have received in the intervening time has convinced us that there is a need for a more succinct way to get started with CVD without requiring someone to read every word in the Guide. To that end, we offer this CVD Quick Start to act as a meta-guide to the Guide.

The Executive Summary contains an overview of the entire document, and is a good place for all readers to become familiar with what's in the guide without necessarily poring over the details. Where you go from there depends on what you're trying to achieve.

- If you're a *researcher*, *vendor*, or *coordinator* trying to coordinate a disclosure and you need help, you might want to start with the 6.10 Troubleshooting Coordinated Vulnerability Disclosure Table to find the problem area(s) you're currently dealing with. From there you can follow the links into the document for more details.
- If you're a *vendor* trying to establish a vendor product security incident response team (PSIRT), you may be interested in 2. Principles of Coordinated Vulnerability Disclosure, 5. Process Variation Points, and 7. Operational Considerations as a starting points. Additionally, you can use the 6.10 Troubleshooting Coordinated Vulnerability Disclosure Table as a rubric of scenarios to consider when planning your operational processes. Appendix E – Disclosure Policy Templates contains links to a number of disclosure policy examples and templates.
- If you're a *coordinator* spinning up your CVD capability, you should become familiar with 2. Principles of Coordinated Vulnerability Disclosure, 3. Roles in CVD, 5. Process Variation Points, and 7. Operational Considerations. The Appendices may also be useful to you.
- If you're a *policy-maker* (or influencer thereof), the sections 1. Introduction , 2. Principles of Coordinated Vulnerability Disclosure, 3. Roles in CVD, and 4. Phases of CVD are probably most useful to you to start, but there are many edge cases in 6.10 Troubleshooting Coordinated Vulnerability Disclosure Table that are worth considering when you're thinking about writing policy that sets out how things are expected to be done. Appendix E – Disclosure Policy Templates contains links to a number of disclosure policy examples and templates.

Of course, we think it's best if you eventually become familiar with the entire document, but hopefully the hints above will help you find the most effective places to start. If you're already familiar with the guide and just want to see what's new, see the update log below.

Recently Updated

- 4.2 Reporting

Sightings

Here is a partial list of places The CERT Guide to Coordinated Vulnerability Disclosure has appeared.

2019-09-17 - Update on the CERT Guide to Coordinated Vulnerability Disclosure - (Software Engineering Institute)

2018-12-14 - Economics of Vulnerability Disclosure (ENISA)

2018-10-23 - The Criticality of Coordinated Disclosure in Modern Cybersecurity (US House Energy and Commerce Committee, Majority Staff)

2018-10-10 - Announcing Arduino's Coordinated Vulnerability Disclosure Policy (Arduino)

2018-09-18 - It Takes a Village: How Hacktivity Can Save Your Company (Atlantic Council)

2018-07-26 - SEI Response to Senate and House Committees regarding Coordinated Vulnerability Disclosure (Software Engineering Institute)

2020-08-19 • updated by Allen D. Householder • view change

- 3.2. Reporter
  2020-06-09 • updated by Art Manion • view change
- Copyright
  2020-04-22 • updated by Allen D. Householder • view change
- Appendix E – Disclosure Policy Templates
  2019-12-12 • updated by Allen D. Householder • view change
- The CERT Guide to Coordinated Vulnerability Disclosure
  2019-12-12 • updated by Allen D. Householder • view change
- 1.1. Coordinated Vulnerability Disclosure is a Process, Not an Event
  2019-12-12 • updated by Allen D. Householder • view change
- Sightings
  2019-09-17 • updated by Allen D. Householder • view change
- Appendix A - On the Internet of Things and Vulnerability Analysis
  2019-09-17 • updated by Allen D. Householder • view change
- 3. Roles in CVD
  2019-09-17 • updated by Allen D. Householder • view change
- role_relationships.png
  2019-09-17 • attached by Allen D. Householder

Show More

Table of contents

2018-07-17 - Letter to SEI from House Committee on Energy and Commerce and Senate Committee on Commerce, Science, and Transportation regarding Coordinated Vulnerability Disclosure (US House & Senate)

2018-07-11 - Senate Testimony regarding Complex Cybersecurity Vulnerabilities: Lessons Learned from Spectre and Meltdown (Art Manion's testimony to the US Senate)

2018-06-28 - Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges (Centre for European Policy Studies)

2018-02-07 - Response to US House Energy and Commerce Committee regarding Meltdown and Spectre (Microsoft)

2018-01-31 - Response to US House Energy and Commerce Committee regarding Meltdown and Spectre (Intel)

2017-11-28 - AMA with Authors of The CERT Guide to Coordinated Vulnerability Disclosure (HackerOne)

2017-10-26 - Your TL;DR Summary of the CERT Guide to Coordinated Vulnerability Disclosure (HackerOne)

2017-08-16 - This one matters, too: Carnegie Mellon issues guide to disclosing software vulnerabilities responsibly (cyberscoop)

2017-08-15 - CERT Guide to Coordinated Vulnerability Disclosure Released (Software Engineering Institute)