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.

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

Appendix F - Additional Resources for Web Vulnerabilities
2021-09-22 • updated by Allen D. Householder • view change
Sightings
2021-07-06 • updated by Allen D. Householder • view change
3.4. Deployer
2021-06-10 • updated by Anonymous • view change
3.4. Deployer
2021-06-10 • updated by Anonymous • view change
3.5. Coordinator
2021-06-10 • updated by Anonymous • view change
3.5. Coordinator
2021-05-25 • updated by Anonymous • view change
4. Phases of CVD
2021-05-25 • updated by Anonymous • view change

Authors:
Allen D. Householder
Garret Wassermann
Art Manion
Chris King

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

CERT/CC Blog post announcing the
publication of the Guide

Sightings

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

2021-06-24 - See Something, Say
Something: Coordinating the Disclosure
of Security Vulnerabilities in Canada
(Cyberspace Policy Exchange)
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)
Table of contents

• Copyright
• Preface
• Acknowledgements
• Executive Summary
• 1. Introduction
  ◦ 1.1. Coordinated Vulnerability Disclosure is a Process, Not an Event
  ◦ 1.2. CVD Context and Terminology Notes
  ◦ 1.3. Why Coordinate Vulnerability Disclosures?
  ◦ 1.4. Previewing the Remainder of this Document
• 2. Principles of Coordinated Vulnerability Disclosure
  ◦ 2.1. Reduce Harm
  ◦ 2.2. Presume Benevolence
  ◦ 2.3. Avoid Surprise
  ◦ 2.4. Incentivize Desired Behavior
  ◦ 2.5. Ethical Considerations
  ◦ 2.6. Process Improvement
  ◦ 2.7. CVD as a Wicked Problem
• 3. Roles in CVD
  ◦ 3.1. Finder
  ◦ 3.2. Reporter
  ◦ 3.3. Vendor
  ◦ 3.4. Deployer
  ◦ 3.5. Coordinator
  ◦ 3.6. Other Roles and Variations
• 4. Phases of CVD
  ◦ 4.1 Discovery
  ◦ 4.2 Reporting
  ◦ 4.3 Validation and Triage
  ◦ 4.4 Remediation
  ◦ 4.5 Gaining Public Awareness
  ◦ 4.6 Promote Deployment
• 5. Process Variation Points
  ◦ 5.1 Choosing a Disclosure Policy
  ◦ 5.2 Disclosure Choices
  ◦ 5.3 Two-Party CVD
  ◦ 5.4 Multiparty CVD
  ◦ 5.5 Response Pacing and Synchronization
  ◦ 5.6 Maintaining Pre-Disclosure Secrecy
  ◦ 5.7 Disclosure Timing
• 6. Troubleshooting CVD
  ◦ 6.1 Unable to Find Vendor Contact
  ◦ 6.2 Unresponsive Vendor
  ◦ 6.3 Somebody Stops Replying
  ◦ 6.4 Intentional or Accidental Leaks
  ◦ 6.5 Independent Discovery
  ◦ 6.6 Active Exploitation
  ◦ 6.7 Relationships that Go Sideways
  ◦ 6.8 Hype, Marketing, and Unwanted Attention
  ◦ 6.9 What to Do When Things Go Wrong
  ◦ 6.10 Troubleshooting Coordinated Vulnerability Disclosure Table
• 7. Operational Considerations
  ◦ 7.1 Tools of the Trade
  ◦ 7.2 Operational Security
  ◦ 7.3 CVD Staffing Considerations
• 8. Open Problems in CVD
  ◦ 8.1 Vulnerability IDs and DBs
  ◦ 8.2 IoT and CVD
• 9. Conclusion
• Appendices
  ◦ Appendix A - On the Internet of Things and Vulnerability Analysis
  ◦ Appendix B - Traffic Light Protocol
  ◦ Appendix C - Sample Vulnerability Report Form
  ◦ Appendix D - Sample Vulnerability Disclosure Document
  ◦ Appendix E - Disclosure Policy Templates
  ◦ Appendix F - Additional Resources for Web Vulnerabilities
• Bibliography
• Sightings
• Recent Changes