The CERT Guide to Coordinated Vulnerability Disclosure

ALLEN HOUSEHOLDER

AUGUST 15, 2017

We are happy to announce the release of the CERTÂ® Guide to Coordinated Vulnerability Disclosure (CVD). The guide provides an introduction to the key concepts, principles, and roles necessary to establish a successful CVD process. It also provides insights into how CVD can go awry and how to respond when it does so.

As a process, CVD is intended to minimize adversary advantage while an information security vulnerability is being mitigated. And it is important to recognize that CVD is a process, not an event. Releasing a patch or publishing a document are important events within the process, but do not define it.

CVD participants can be thought of as repeatedly asking these questions: What actions should I take in response to knowledge of this vulnerability in this product? Who else needs to know what, and when do they need to know it? The CVD process for a vulnerability ends when the answers to these questions are nothing, and no one.

If we have learned anything in nearly three decades of coordinating vulnerability reports at the CERT/CC, it is that there is no single right answer to many of the questions and controversies surrounding the disclosure of information about software and system vulnerabilities. The CERT Guide to CVD is a summary of what we know about a complex social process that surrounds humans trying to make the software and systems they use more secure. It's about what to do (and what not to) when you find a vulnerability, or when you find out about a vulnerability. It's written for vulnerability analysts, security researchers, developers, and deployers; it's for both technical staff and their management alike. While we discuss a variety of roles that play a part in the process, we intentionally chose not to focus on any one role; instead we wrote for any party that might find itself engaged in coordinating a vulnerability disclosure.

In a sense, this report is a travel guide for what might seem a foreign territory. Maybe you've passed through once or twice. Maybe you've only heard about the bad parts. You may be uncertain of what to do next, nervous about making a mistake, or even fearful of what might befall you. If you count yourself as one of those individuals, we want to reassure you that you are not alone; you are not the first to experience events like these or even your reaction to them. We're locals. We've been doing this for a while. Here's what we know.

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.

The CERTÂ® Guide to Coordinated Vulnerability Disclosure is available in the SEI Digital Library.

SHARE

WRITTEN BY

Allen Householder

AUTHOR PAGE

DIGITAL LIBRARY PUBLICATIONS

SEND A MESSAGE TO ALLEN HOUSEHOLDER

MORE BY THE AUTHOR

Prioritizing Vulnerability Response with a Stakeholder-Specific Vulnerability Categorization

DECEMBER 5, 2019 • BY ALLEN HOUSEHOLDER

Update on the CERT Guide to Coordinated Vulnerability Disclosure

SEPTEMBER 16, 2019 • BY ALLEN HOUSEHOLDER

Comments on Voluntary Voting System Guidelines 2.0 Principles and Guidelines

JUNE 14, 2019 • BY ALLEN HOUSEHOLDER , DEANA SHICK , JONATHAN SPRING , ART MANION

Announcing CERT Basic Fuzzing Framework Version 2.8

OCTOBER 5, 2016 • BY ALLEN HOUSEHOLDER

Vulnerability IDs, Fast and Slow

MARCH 11, 2016 • BY ALLEN HOUSEHOLDER

Get updates on our latest work.

Each week, our researchers write about the latest in software engineering, cybersecurity and artificial intelligence. Sign up to get the latest post sent to your inbox the day it's published.

Subscribe

Get our RSS feed

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800