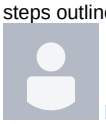
Vulnerability Analysis

Vulnerability analysis at the CERT Coordination Center® (CERT/CC) consists of a variety of efforts, with primary focus on coordinating vulnerability disclosure and developing vulnerability discovery tools and techniques. Publicly available resources include:

- Public vulnerability information: Vulnerability Notes and vulnerability data archive
- Coordination and disclosure guidance for security researchers and vendors
- The CERT Guide to Coordinated Vulnerability Disclosure in its entirety
- Vulnerability Disclosure Policy Templates for use in creating your own customized disclosure policy
- Vulnerability Reporting Form (please be familiar with the guidelines before reporting)
- Open-source vulnerability discovery and analysis tools
    - CERT BFF - Basic Fuzzing Framework — The CERT Basic Fuzzing Framework (BFF) is a software testing tool that finds defects in applications that run on the Linux and Mac OS X platforms. BFF performs mutational fuzzing on software that consumes file input.
    - CERT FOE - Failure Observation Engine — The CERT Failure Observation Engine (FOE) is a software testing tool that finds defects in applications that run on the Windows platform. FOE performs mutational fuzzing on software that consumes file input.
    - CERT Tapioca — CERT Tapioca is a network-layer man-in-the-middle (MITM) proxy framework based on mitmproxy http://mitmproxy.org/. CERT Tapioca is installable on Red Hat Enterprise Linux, CentOS, Fedora, Ubuntu, OpenSUSE, and Raspbian.
    - CERT Triage Tools — The CERT Triage Tools project has been transitioned to the GDB 'exploitable' plugin https://github.com/jfoote/exploitable project on GitHub.
    - CERT Vulnerability Data Archive and Tools — The CERT Vulnerability Data Archive contains nearly all of the non-sensitive vulnerability data collected by the CERT/CC, from the inception of the vulnerability notes database (approximately May 1998) to the date the archive was prepared, as noted above in the Change Log.
    - Dranzer — Dranzer is a tool that enables users to examine effective techniques for fuzz testing ActiveX controls.

Recent Blog Posts


Kerberos relaying with krbrelayx and mitm6
Will Dormann posted on Feb 24, 2022
Overview Dirk-jan Mollema published a blog post that shows how an attacker on the same (V)LAN as a machine connected to an active directory where an AD CS server is present can obtain a kerberos ticket to impersonate a domain admin on the victim system: https://dirkjanm.io/relaying-kerberos-over-dns-with-krbrelayx-and-mitm6/ https://dirkjanm.io/relaying-kerberos-over-dns-with-krbrelayx-and-mitm6/ Using the steps outlined, an attacker can execute code with SYSTEM privileges on the victim system.…


Finding Privilege Escalation Vulnerabilities in Windows using Process Monitor
Will Dormann posted on Jun 21, 2021
Overview This post will explain how to find privilege escalation vuls on Windows that no one appears to be looking for, because it's been pretty easy to find a bunch of them. After explaining how to find them, I'll introduce some defenses that can partly mitigate the problem in different ways. But what I'd like to see change is for developers to start looking for these vuls in the way I describe so that they stop introducing them in the first place.…

Recently Updated

VINCE API
2022-03-09 • updated by Will Dormann • view change
CERT FOE - Failure Observation Engine
2022-03-09 • updated by Will Dormann • view change
For Vendors
2022-03-02 • updated by Emily Sarneso • view change
Vulnerability Note API
2022-01-05 • updated by Emily Sarneso • view change
Vulnerability Note Help
2021-12-21 • updated by Art Manion • view change
CERT Advisory CA-2003-04 MS-SQL Server Worm
2021-10-25 • updated by Art Manion • view change
CERT Tech Tips
2021-10-08 • updated by Allen D. Householder • view change
CERT Incident Notes
2021-10-08 • updated by Allen D. Householder • view change
CERT Advisories
2021-10-08 • updated by Allen D. Householder • view change
CERT Coordination Center Historical Documents
2021-10-08 • updated by Allen D. Householder • view change