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
- The CERT Guide to Coordinated Vulnerability Disclosure, including
  - Vulnerability Disclosure Policy Templates for use in creating your own customized disclosure policy
  - Coordination and disclosure guidance for security researchers and vendors
- Vulnerability Reporting Form (please be familiar with the guidelines before reporting)
- Open-source vulnerability discovery and analysis tools, including
  - The CERT Basic Fuzzing Framework is a software testing tool that finds defects in applications that run on Linux, macOS, and Windows platforms.
  - CERT Tapioca is a network-layer man-in-the-middle (MITM) proxy framework based on mitmproxy.
  - Dranzer is a tool that enables users to examine effective techniques for fuzz testing ActiveX controls

Recent Blog Posts

Probably Don't Rely on EPSS Yet
Jonathan Spring posted on Jun 06, 2022
Author's Note: This post was updated on June 9, 2022, to correct factual errors including references to Kenna Security instead of AlienVault and Fortinet. This post was updated on June 14, 2022, to edit content to reflect the publication of the EPSS FAQ https://www.first.org/epss/faq on June 10, 2022. Vulnerability management https://en.wikipedia.org/wiki/Vulnerability_management involves discovering, analyzing, and handling new or reported security vulnerabilities in information systems."

Finding Privilege Escalation Vulnerabilities in Windows using Process Monitor
user-9a25e 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...

Kerberos relaying with krbrelayx and mitm6
user-9a25e 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...