Security Experts on Open Source
Security Experts on Open Source

Moderator:
Karl MacMillan
Director of Core Technology, Tresys Technology

Panelists:
Daniel Risacher
Associate Director, Enterprise Services and Integration, Department of Defense CIO

Daniel Walsh
Principal Software Engineer, SELinux Technical Lead, Red Hat

John Banghart
SCAP Validation Program Manager, National Institute of Standards and Technology

Steve Battista
Lead Information Security Scientist, MITRE
Karl MacMillan
Director of Core Technology
Tresys Technology
Daniel Risacher

Associate Director, Enterprise Services and Integration
Department of Defense CIO
Before Virtualization

User Space

Web App

Host Kernel

User Space

DNS Server

Host Kernel
Good tools for detecting network attacks

[Diagram showing network architecture with User Space, Host Kernel, Web App, and DNS Server.]
After Virtualization

- Host Kernel
- Host Hardware
  - memory, storage, etc.

- User Space
  - Web App

- User Space
  - DNS Server
What could possibly go wrong?
After Virtualization

User Space

Web App

Host Kernel

User Space

DNS Server

Host Kernel

Host Kernel

Host Hardware
memory, storage, etc.
Hypervisor vulnerabilities

Not theoretical
Evolving field
Potentially huge payoffs
Xen already compromised...
Adventures with a certain Xen vulnerability (in the PVFB backend)

version 1.0

Rafal Wojtczuk
Invisible Things Lab
rafal@invisiblethingslab.com

October 14, 2008

1 Introduction

This paper documents the research by the author to understand the nature of and write an exploit for the CVE-2008-1943 vulnerability[1]. In x86_32 architecture case, the exploit can escape from a Xen PV guest to dom0. The challenges posed by SELinux are taken into consideration. Some techniques that failed to succeed with the default configuration (particularly, in x86_64 case) are also documented, because of their potential usefulness in other cases.

The exploits were written for Fedora 8 Linux distribution as dom0; it is the latest release of this popular distribution that comes with a dom0-capable kernel. Additionally, Xen 3.2.0 rpms (retrieved from xen.org site) were installed to the test dom0 machine.

2 The nature of the vulnerability
Who is the weakest link?

Host Kernel

Host Hardware
memory, storage, etc.
Enter SELinux...

SELinux is all about labeling
Processes get labels
Virtual machines are processes!!!
Files/Devices Get Labels
Virtual images are stored on files/devices!!!!
Kernel Enforces these Rules.
Libvirt – Dynamic Labeling in action

svirt_t:MCS1

svirt_t:MCS2

svirt_image_t:MCS1

svirt_image_t:MCS2

User Space

Web App

Host Kernel

DNS Server

User Space

Host Kernel

Host Kernel

SELinux

Host Hardware
memory, storage, etc.
John Banghart

SCAP Validation Program Manager
National Institute of Standards and Technology
References

John Banghart – NIST – john.banghart@nist.gov

SCAP Website – http://scap.nist.gov
National Checklist Program (NCP) – http://checklists.nist.gov
- DRAFT SP 800-126: SCAP Specification
- DRAFT IR 7511: SCAP Derived Test Requirements
Steve Battista

Lead Information Security Scientist
MITRE
Panel Discussion
Questions?

Tell us what you think:
Complete the survey