Security & Ubuntu

PA Hackers

September 25, 2019

Mike Salvatore
ESM Tech Lead/Security Engineer

CANONICAL ubuntu

Who Am I?

- Education
  - B.S. Electrical Engineering, Rutgers University
  - M.S. Cybersecurity, Johns Hopkins University
- Current employment
  - Ubuntu Security Team at Canonical
- Contact
  - mike.salvatore@canoncal.com
  - msalvatore on the freenode IRC network
  - @L0n3_W0lf on the PA Hackers Slack

Bad News
Good News
Good News
Bad News

Bad News

PA Hackers had a number of presenters tonight who, due to a variety of circumstances, were unable to make it.

Good News

I volunteered to fill in and discuss how Canonical and Ubuntu approach security.

Good News

This is not a BSides presentation, so, instead of a BSides preview, you’ll get to see a presentation that’s not available at the upcoming BSides Harrisburg event.

Bad News

This was thrown together last minute. You’ll have to suffer through how unprepared I am to give this presentation.

Contents

01 What are stable releases?

02 What is Ubuntu?

03 How does Ubuntu keep its packages secure?

04 Security Features in Ubuntu

05 Getting Involved with the Ubuntu Security Team.

Stable Releases
vs.
Rolling Releases

What is a Stable Release?

- Also called point release, standard release, or versioned release
- The goal of a stable release is to provide developers and users with a platform that changes as minimally as possible.
- “Stability” in stable release doesn’t necessarily refer to the likelihood of the system to crash (though that is a byproduct), but rather to the stability of ABI/API, availability of libraries, etc.

What is a Rolling Release?

- Rolling release is a development model where updates are continually released as they become available.
- Gives you access to the most cutting edge features that stable releases may not have released yet
- Minimizes the number of CVEs affecting your system
- Higher risk of bugs and breakage

Which is Better?

- Do you want the most cutting edge features? Rolling release is better.
- Do you have custom applications that rely on specific versions of software packaged with your OS? Older hardware? Stable release might be better.

What is Ubuntu?

Ubuntu is a Linux distro based on Debian

- Debian is a very conservative distribution, i.e. very very stable.
  - New stable releases of Debian are released approximately every 2 years, though there is no set schedule.
- In contrast, new versions of Ubuntu are released every 6 months.

Overview of Debian Releases

- Debian provides 3 releases (https://www.debian.org/releases/)
  - Stable - The stable distribution contains the latest officially released distribution of Debian.
  - Testing - The testing distribution contains packages that haven't been accepted into a stable release yet, but they are in the queue for that. The main advantage of using this distribution is that it has more recent versions of software.
  - Unstable - The unstable distribution is where active development of Debian occurs. Generally, this distribution is run by developers and those who like to live on the edge.

What is Ubuntu Made Of?

- Ubuntu releases include packages from all 3 debian releases.
- By incorporating packages from Debian Testing and Debian Unstable, Ubuntu can provide newer software than Debian Stable.
- Packages in Ubuntu are tested to ensure compatibility and supported for a predetermined period of time
- Debian does not necessarily provide any support for packages in Testing or Unstable
- Ubuntu provides its own interface and themes, installer, as well as some other packages that are focused on improving user experience.

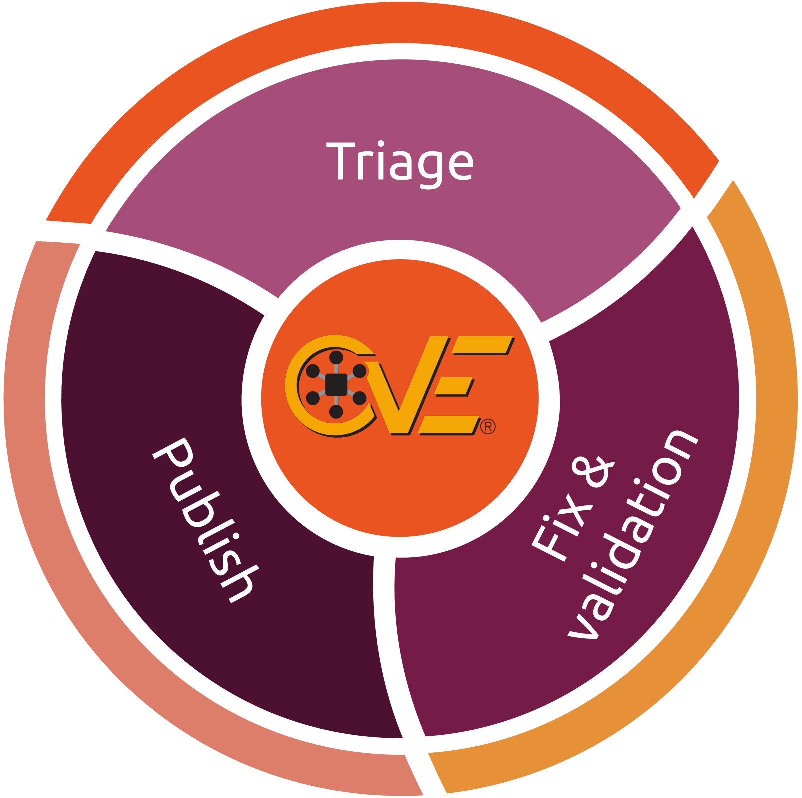
Supporting Ubuntu

- Ubuntu provides security updates and some bugfix/feature updates to supported Ubuntu releases
- A new version of Ubuntu is released every 6 months
- Most are supported for 9 months
- Every 2 years, in April, Ubuntu puts out a Long-Term Support (LTS) release
    - Trusty 14.04
    - Xenial 16.04
    - Bionic 18.04
- LTS releases are supported for 5 years

Backporting Security Patches

- Stable release distros (including Ubuntu) backport security fixes from upstream projects to address security vulnerabilities in their packages.
- This allows the release to remain stable and secure.
- Security patches are released continuously for Ubuntu packages (i.e. we don’t observe any schedule like “Patch Tuesday”, but make security fixes available in real time)

Secure By Process



https://cve.mitre.org/
https://usn.ubuntu.com/

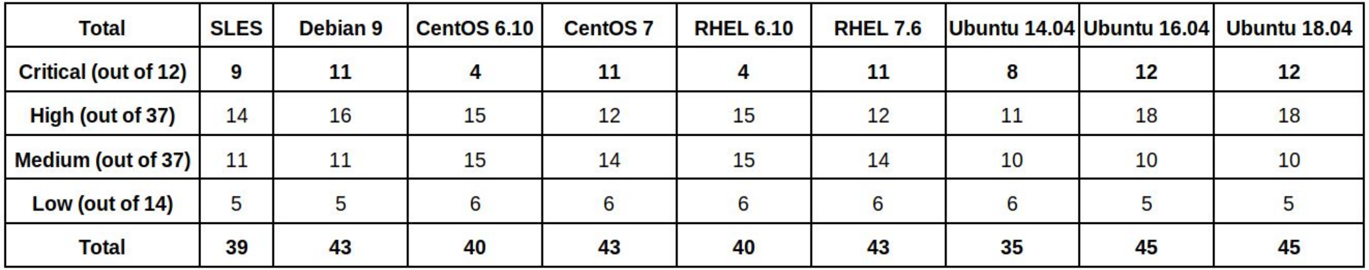
Ubuntu Security Features

Compile-time Security Options

- Stack protector
- Heap Protector
- ASLR/PIE
- And more!

Kernel Security Features

Ubuntu enables a number of kernel security features out of the box.



Total	SLES	Debian 9	CentOS 6.10	CentOS 7	RHEL 6.10	RHEL 7.6	Ubuntu 14.04	Ubuntu 16.04	Ubuntu 18.04
Critical (out of 12)	**9**	**11**	**4**	**11**	**4**	**11**	**8**	**12**	**12**
High (out of 37)	14	16	15	12	15	12	11	18	18
Medium (out of 37)	11	11	15	14	15	14	10	10	10
Low (out of 14)	5	5	6	6	6	6	6	5	5
Total	**39**	**43**	**40**	**43**	**40**	**43**	**35**	**45**	**45**

A comparison of kernel security features in different Linux distros

Source: https://capsule8.com/blog/millions-of-binaries-later-a-look-into-linux-hardening-in-the-wild/

Firewall

- Most Linux distros support firewalls
  - iptables
  - nftables
  - bpfilter
- Some distros provide easy-to-use tools to help configure firewalls
  - Ubuntu provides UFW
  - SuSE provides tools to configure the firewall through YaST

AppArmor

- AppArmor is a MAC security system built upon the Linux Security Module (LSM).
- AppArmor confines the behaviour of individual programs based on a set of policies defined by an administrator. In other words, AppArmor allows administrators to apply the principle of least privilege at the application level.
- For more information, see https://ubuntu.com/engage/apparmor-intro

Pockets: Security and Updates

- Ubuntu makes it possible to apply only security fixes to your systems. This allows systems to stay secure while maximizing security.
- Ubuntu publishes security fixes to the -security pocket and important bug fixes to the -updates pocket
  - -updates includes things that have gone through the StableReleaseUpdates process, and contain various important bug fixes. Anything built for "-updates" is built on top of whichever version of a package is newest between "-updates" and "-security", so that nothing in "-updates" will introduce security regressions.
  - -security includes only updated packages that contain security-related fixes, and are built to not require anything from "-updates". Anything built for "-security" is built on top of whichever version of a package is newest between "-updates" and "-security", so that nothing in "-security" will introduce bug regressions.
  - https://wiki.ubuntu.com/SecurityTeam/FAQ

Upstreaming New Security Features (Example)

- We take a proactive approach to security and develop new security features when possible.

Can you spot the vulnerability?

```
#!/bin/bash
echo “Hello World!” > /tmp/hello_world.txt
cat /tmp/hello_world.txt
rm /tmp/hello_world.txt
```

Upstreaming New Security Features (Example)

Can you spot the vulnerability?

```
#!/bin/bash
echo “Hello World!” > /tmp/hello_world.txt
cat /tmp/hello_world.txt
rm /tmp/hello_world.txt
```

In Linux, /tmp is a world read/writable directory. Because the above script writes to a predictable file name, an attacker could create a /tmp/hello_world.txt as a symlink (analogous to a shortcut in Windows). When this script is run, the string “Hello World” will be written to the target of the symlink. This could be used to overwrite system configuration files resulting in a denial of service or other compromise.

This is called a time-of-check to time-of-use (TOCTOU) attack.

https://lwn.net/Articles/472071/

Upstreaming New Security Features (Example)

In order to prevent TOCTOU attacks, the Linux kernel was modified by Kees Cook who was, at the time, a member of the Ubuntu Security Team.

In Ubuntu 10.10 and later, symlinks in world-writable sticky directories (e.g. /tmp) cannot be followed if the follower and directory owner do not match the symlink owner.

https://lwn.net/Articles/472071/

Certified Compliance

Federal Information Processing Standard (FIPS) 140-2 Level 1

Common Criteria EAL2 (ISO/IEC IS 15408)

Security Technical Implementation Guide (STIG)

Center for Internet Security (CIS) benchmark

https://ubuntu.com/blog/canonicals-security-certifications

Is Ubuntu the Most Secure Linux Distro?

- This is not a very good question.
- Security can be measured by many different criteria and different Linux distros have different use cases.
- We can say that security is a top priority in Ubuntu. Here is a list of security features in Ubuntu: https://wiki.ubuntu.com/Security/Features
- Results of one independent analysis:
  - "Our experiments indicate that Ubuntu 18.04 shows the largest adoption of OS and application-level mitigations…"
  - "On the other hand, OpenSUSE 12.4, CentOS 7 and RHEL 7 also deploy common hardening schemes, and show wider adoption stack-clash mitigations while shipping a much more tight-knit set of packages by default."
  - Source: https://capsule8.com/blog/millions-of-binaries-later-a-look-into-linux-hardening-in-the-wild/

Getting Involved with the Ubuntu Security Team

Ways to Get Involved

- Contributing to open source projects is an excellent way to improve your skills and build your resume.
- If you're interested in Linux security, application security, secure coding, or vulnerability research, you might enjoy
- Here's a post from my blog* that dives more deeply into why you should contribute to open source projects: https://salvatoresecurity.com/breaking-into-cybersecurity-with-open-source/

* My blog, salvatoresecurity.com, is in no way affiliated with Canonical or Ubuntu. The views, thoughts, and opinions expressed therein belong solely to me, the author, and not necessarily my employer.

Ways to Get Involved

- Join us on #ubuntu-hardened on irc.freenode.net
    - Offer to test packages with security updates
- Write Documentation
- Find security bugs
- Triage security bugs
- Fix security bugs
- For more information, see https://wiki.ubuntu.com/SecurityTeam/GettingInvolved

Thank you. Questions?