Surviving in the World of Holes

IVA GLAZAROVÁ, LINUX DAYS 2018

Speaker Introduction

- Iva Glazarová
- Fresh graduate
- Working in MSD, Global Infrastructure Operations
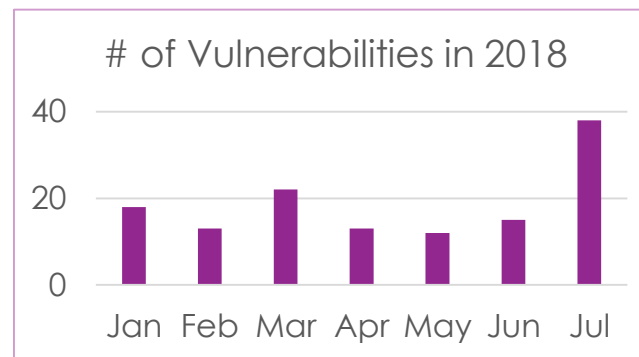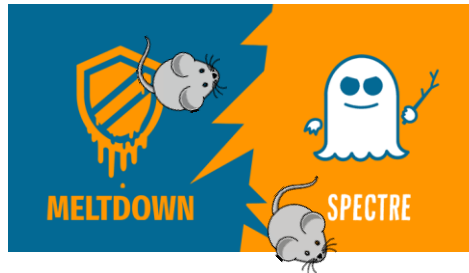 - Unix/Linux Team
  - https://www.msdit.cz/

Agenda & Topic Introduction

- Problem Statement
- Vulnerability Management
- Proactive Approach
- Corporate Global Challenges

Problem Statement

- Linux Vulnerabilities
  - Yearly in 2017: 453
  - Vulneribilities every month – stay current
- Safety vs. Agile
- Approach
  - Proactive
  - Reactive
- Vulnerability management

Year	# of Vulnerabilities
2014	133
2015	86
2016	217
2017	453
2018	131

# of Vulnerabilities in 2018

Linux Kernel Vulnerability Statistics

Stay up to date – patch, patch, patch

Product, package

Red Hat Enterprise Linux 7 (z-stream) kernel

CVE-2017-5754

RHSA-2018-0007

- ▶ CVE, NVD
- ▶ Patch them all!
- ▶ Scan > Prioritize > Assess > Report > Fix > Verify

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.0
Critical	9.0-10.0

CVSS v3.0 Ratings

Reducing Attack Surface

- Unify environment landscape
- Customize server build
  - Do not start services your are not using
  - Privilage account management
  - Multi-factor authentification
  - Do not use default ports

Be ready for Day Zero Vulnerability

- Firewall
- Whitelisting software
- Segmentation: HW, Network
- Do not mess with strangers (USB)
- Intrusion detection system

# Corporate Global Challenges

- Systems supporting global applications running 24/7
- 3rd party access to network
- Diverse & complex environment
- Decision making - getting approvals
- Highly regulated environment

Summary & Highlights

▶ Company without patching strategy is like truck company without oil change plan

▶ Proactive approach gives you more time for innovation and added value things

▶ No patching means disaster awaiting
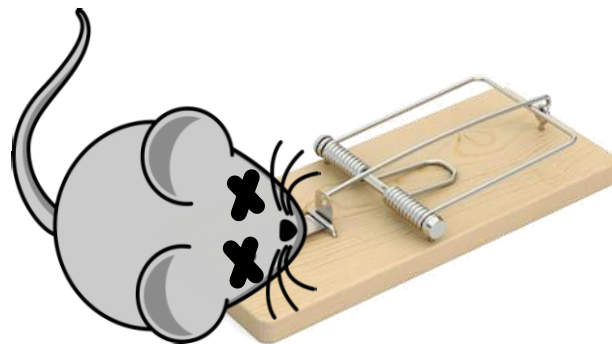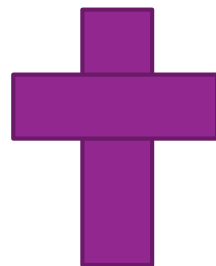
Penguin can't get out of the hole!

323K views   👍 156   👎 79   ➤ SHARE   ≡+   ...

Thank you for your attention

Meet my team

Survived in the world of holes