Red Hat Product Security

Understanding and Mitigating Security Risk

Langley Rock
Sr. Program Mgr., Product Security
lrock@redhat.com

WIFI INFO
Westin_CONFERENCE
Redhat2019

BE SOCIAL #SECURITYSYMPOSIUM

Red Hat

AGENDA

- 2018 Risk Report
- Product Security Vision, Organization and Team Structure
- Dealing with and Rating Vulnerabilities
- Customer Security Awareness Events
- Pop Quiz


IN 2018
745
Red Hat
SECURITY ADVISORIES
1,272
CVEs
ADDRESSED
Source: 2018 Red Hat Product Security Risk Report, February 2019. red.ht/2018riskreport

Red Hat

2018 RISK REPORT

- 1,272 CVEs were addressed throughout 2018, an 11% increase from 2017
- 745 Red Hat Security Advisories were issued, a continued increase year-over-year
- 3,774 security issues were reported to Red Hat Product Security (nearly x2 vs 2015)
- 111 Critical advisories addressing 57 Critical vulnerabilities
- 80% of Critical issues were addressed within 1 week
- 38% of Critical issues were addressed within 1 business day

https://red.ht/2018riskreport

Red Hat

RED HAT PRODUCT SECURITY VISION

“We believe that everyone, everywhere, is entitled to quality information needed to mitigate security and privacy risk as well as the access to do so. We strive to protect communities of customers, contributors, and partners from digital security threats. We believe open source principles are the best way to achieve this.”

Red Hat

CUSTOMER EXPERIENCE & ENGAGEMENT

Red Hat Customer Experience and Engagement is strategically positioned within the engineering organization, creating a more direct route for customer-driven product improvements and faster engineering related fixes.

PRODUCTS AND TECHNOLOGIES

CUSTOMER EXPERIENCE AND ENGAGEMENT

Customer Platform	Development & Operations	Quality Engineering	Voice of the Customer
Product Security	Global Support and Customer Success	CEE Strategic Services	Customer Content Services

CUSTOMER PORTAL

Red Hat

RED HAT PRODUCT SECURITY TEAM STRUCTURE AND RESPONSIBILITIES

PSIRT

- Vulnerability triage, analysis, intelligence and monitoring, report intake, and documentation
- Product review and audits
- Technology guidance
- Research and upstream community engagement

ASSURANCE

- Stakeholder management
- Product governance
- Critical issue incident management
- Internal/External communications and documentation

PROCESS & INFORMATION ENABLEMENT

- Internal tooling coordination
- Insights rules development
- Security metrics

Red Hat

WHAT IS A SECURITY VULNERABILITY?

As you know, a security vulnerability is a software, hardware or firmware flaw that could allow an attacker to interact with a system in a way it is not supposed to.

The one that keep us up at night are those which

- Compromise sensitive data (keys, financial information, customer information)
- Allow the execution arbitrary code on remote systems
- Denial of availability for mission-critical services

The severity of a vulnerability is determined by:

- the likelihood of a vulnerability being exploited
- the impact to the system or asset that is exposed
- the value of that system or asset

RED HAT PRODUCT SECURITY

Red Hat Product Security works constantly to ensure timely and appropriate security fixes for our supported products and services. Our security response process is carefully designed and thoroughly validated to manage vulnerabilities.

Our team ensures product and service security by:

Investigating issues and then identifying affected products

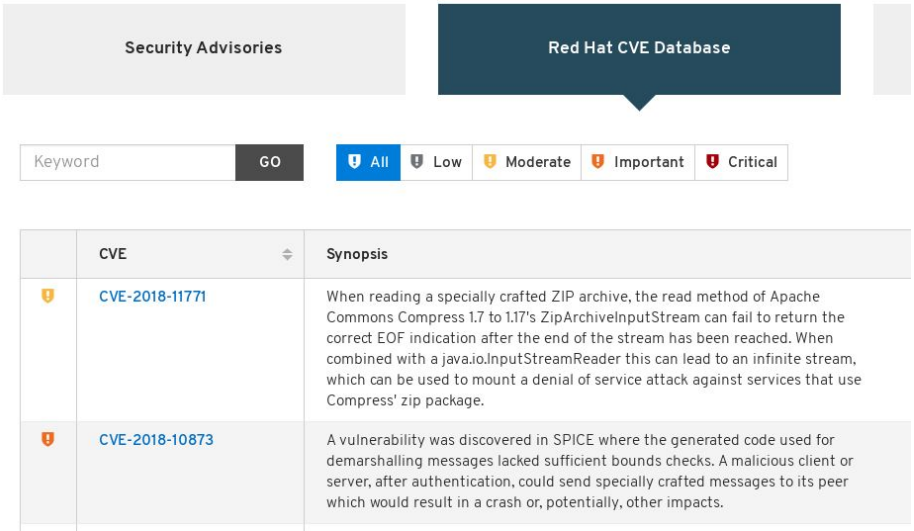
Evaluating the impact

Determining any necessary remediation actions

Communicate issues and remediation to customers

Red Hat

COMMON VULNERABILITIES AND EXPOSURES



CVEs provide a transparent way to identify and track security issues

- Red Hat Product Security assigns CVEs to every security issue that impacts our products
- CVEs may be assigned retroactively to previous bugs that are found to be security-relevant
- All CVEs affecting Red Hat products are listed in our public database

https://access.redhat.com/security/security-updates/#/cve

Red Hat

CVE IN-DEPTH

CVE's all contain a unique identifier

CVE-2019-5736

CVE's all contain a brief description

runc: Execution of malicious containers allows for container escape and access to host filesystem

CVE's all include relevant references

https://access.redhat.com/security/cve/cve-2019-5736

https://bugzilla.redhat.com/show_bug.cgi?id=1664908

https://cve.mitre.org/about/index.html

Red Hat

HOW TO SCORE USING CVSS

Determine the base score

There are 8 dimensions of the flaw to review:

- Attack Vector
- Attack Complexity
- Privileges Required
- User Interaction
- Scope
- Confidentiality
- Integrity
- Availability

Each is rated (mostly) on a High-Low-None scale

Pro Tip: You can customize scoring based on your environment

Temporal

- Exploit Code Maturity
- Remediation Level
- Report Confidence

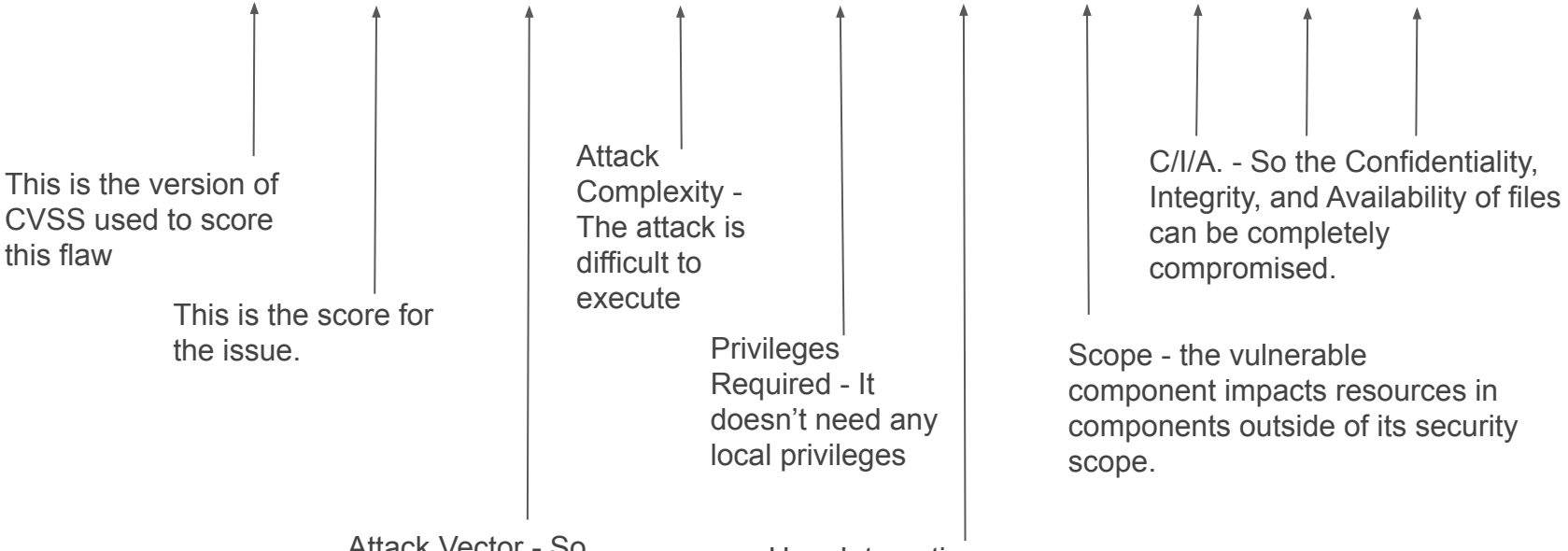
Environmental

- CIA Requirement
- Modified base score dimension

Red Hat

WHAT DOES A CVSS SCORE LOOK LIKE?

CVSS:3.0- 7.7/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H



https://www.first.org/cvss/calculator/3.0

Red Hat

IF YOU LEAVE WITH ONE THING...

CVSS != RISK

CVSS QUANTIFIES SEVERITY

CVSS is just one data point in risk assessment.

Factors that Red Hat Considers

- Is the flaw even applicable to a Red Hat product?
- How is the code built in Red Hat products (compiler flags, etc)?
- Does the ‘fix’ break compatibility?
- Are there built-in mitigations (SELinux) that reduce risk?
- What is the lifecycle of the affected product?

WHY IS CVSS IMPORTANT?

CVSS scoring provides a method to prioritize which vulnerabilities should get addressed first based on chosen criteria

What risk factors do Customers need to consider?

- How, and where, are the affected products deployed?
- Performance trade-off versus risk assessment
- Regulatory compliance requirements versus actual risk

WHERE DO THE SCORES COME FROM?

National Vulnerability Database - NVD	*vs*	**Red Hat**
Issue not necessarily scored by technology-expert		Issue scored by Red Hat Product Security
Score does not take into account things like compiler switches, default hardening, nor tools like SELinux		Score accounts for build and configuration options that Red Hat uses
No testing of reproducer against running environment		Score reflects actual testing and triage of the issue and specific products affected
Generic score does not take into account different configurations or Operating Systems		Scoring is specific to configuration or Operating System

Red Hat

RED HAT SEVERITY RATINGS

CRITICAL

A remote unauthenticated user can execute arbitrary code

Does not require user interaction

I.e. Worms

IMPORTANT

Allows local users to gain privileges

Unauthenticated remote users can view resources

Authenticated remote users can execute arbitrary code

MODERATE

Vulnerabilities are more difficult to exploit

Are exploitable via an unlikely configuration

LOW

Unlikely circumstances required to exploit

Impact is of minimal consequence

https://access.redhat.com/security/updates/classification/

Red Hat

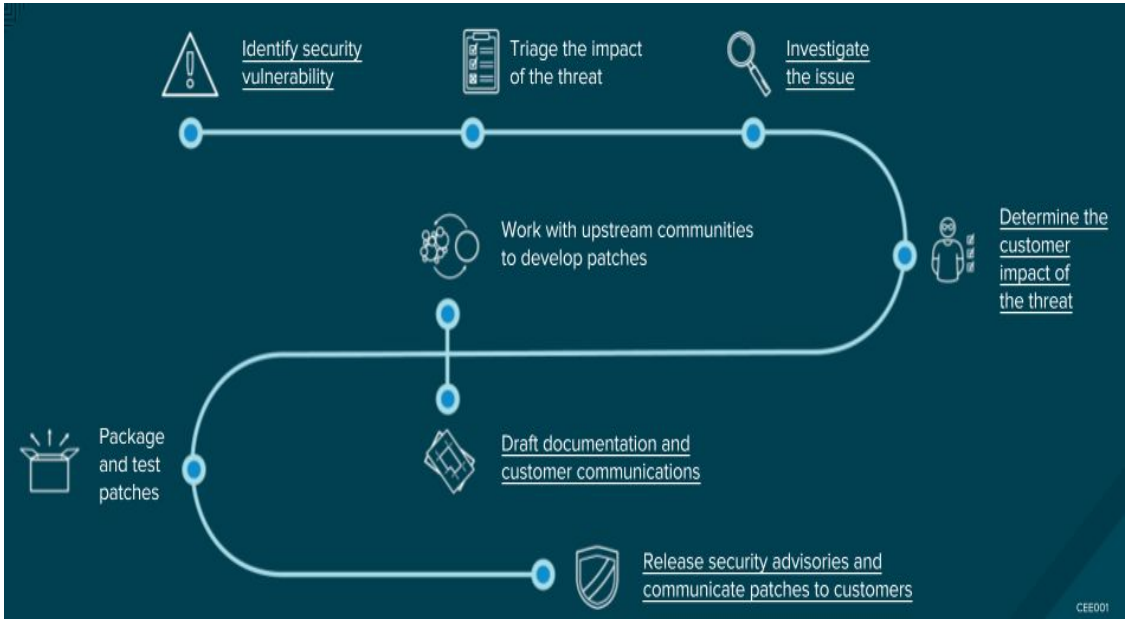
COORDINATED VULNERABILITY DISCLOSURE

- Red Hat is part of a large group of vendor and community security teams
- We use a process called Coordinated Vulnerability Disclosure
- The goal is to protect customers and the larger global computing community
- Red Hat works with the issue reporter on how they want the issue to be handled and how long to keep it under embargo

https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

Red Hat

CUSTOMER SECURITY AWARENESS EVENTS



CSAWs are specialized activities designed to manage high-touch events:

- Critical or Important severity
- Extensive media attention
- Active exploitation

CSAW process helps ensure:

- Expedited solutions
- Transparency and completeness of customer-facing communication

https://access.redhat.com/articles/2968471

Red Hat

WE DON’T BELIEVE THE HYPE

- A vulnerability may get a name, a logo, or press attention, but that doesn’t mean it poses greater risk
- Red Hat tells you **which branded vulnerabilities matter and which are less severe than they are made out to be**

Red Hat

POP QUIZ!!!

- How many of these vulnerabilities was/were rated CRITICAL

  Don’t believe the hype. All were rated IMPORTANT, except for one…

Red Hat

POP QUIZ!!!

CVE-2014-6271 Shellshock

https://access.redhat.com/security/vulnerabilities/shellshock

POP QUIZ!!!

- Which of these has the highest **CVSS risk**

Red Hat

POP QUIZ!!!

CVSS != RISK

Red Hat

REPORTING SECURITY VULNERABILITIES

If you think you have identified a security vulnerability, contact Product Security at secalert@redhat.com

Product Security will analyze and appropriately handle any reports we receive.

In the case of upstream projects, Product Security will help coordinate additional conversations and impose an embargo if required.

Red Hat

QUESTIONS?

Thank you to our partner