Red Hat Product Security

Understanding and Mitigating Security Risk

Vincent Danen
Senior Director, Product Security
vdanen@redhat.com

Delta_CONFERENCE /
REDHAT2019

WHO I AM

VINCENT DANEN
Senior Director, Product Security

- Twenty years working with Open Source, the last 18 of which working with Open Source security
- Ten years at Red Hat
- 100% Alberta born and raised

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

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

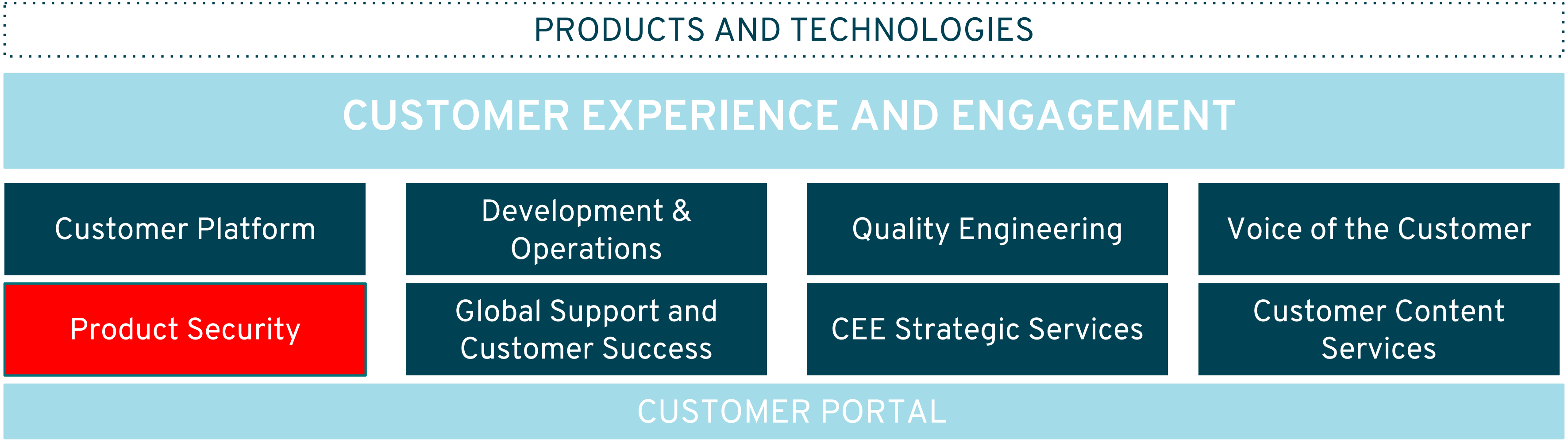
https://red.ht/2018riskreport

RED HAT 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.”

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 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

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

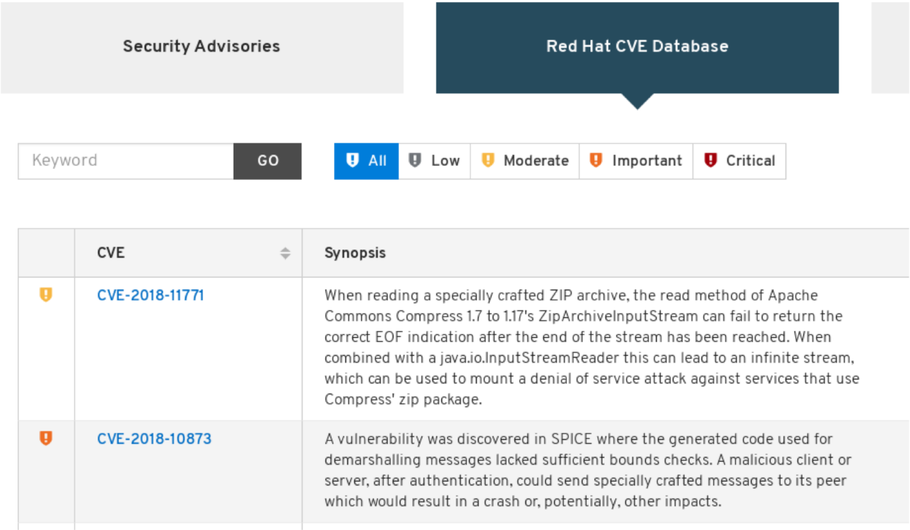
RED HAT PRODUCT SECURITY

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

COMMON VULNERABILITIES AND EXPOSURES



	CVE	Synopsis
	CVE-2018-11771	When reading a specially crafted ZIP archive, the read method of Apache Commons Compress 1.7 to 1.17's ZipArchiveInputStream can fail to return the correct EOF indication after the end of the stream has been reached. When combined with a java.io.InputStreamReader this can lead to an infinite stream, which can be used to mount a denial of service attack against services that use Compress' zip package.
	CVE-2018-10873	A vulnerability was discovered in SPICE where the generated code used for demarshalling messages lacked sufficient bounds checks. A malicious client or server, after authentication, could send specially crafted messages to its peer which would result in a crash or, potentially, other impacts.

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

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

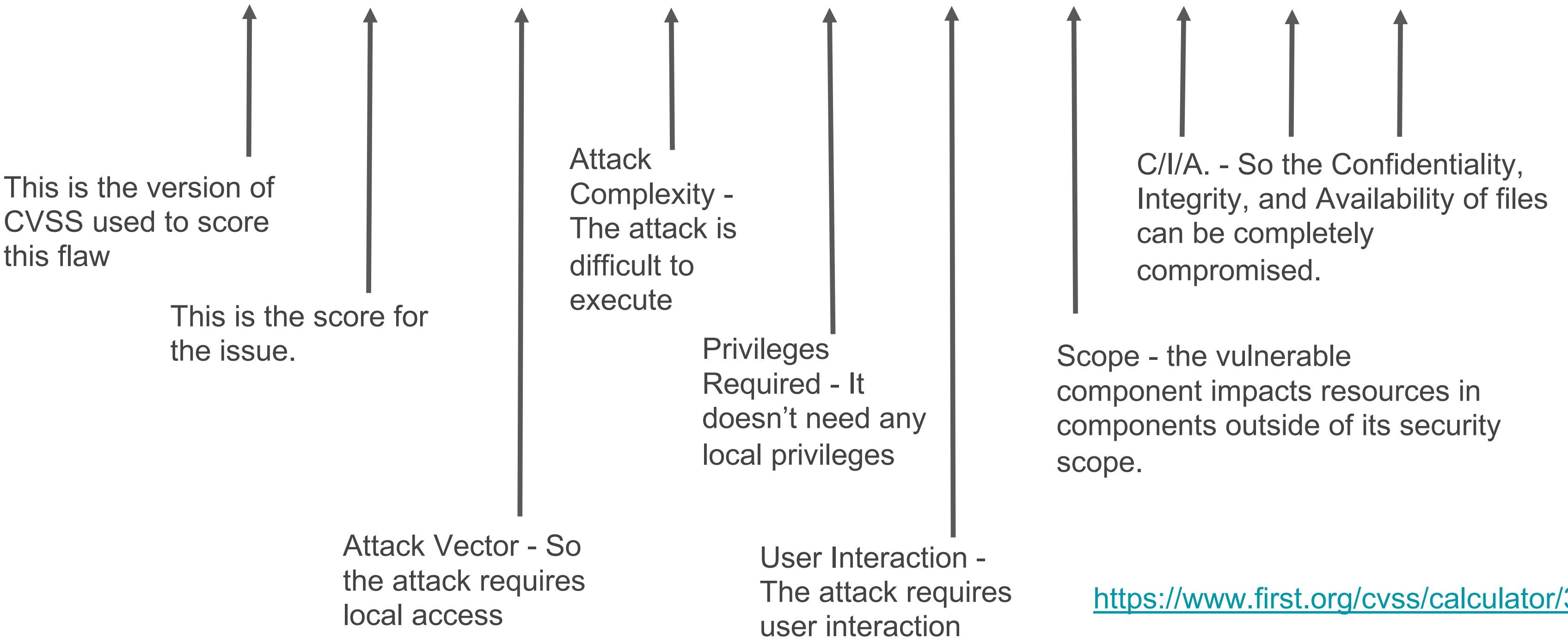
- Exploit Code Maturity
- Remediation Level
- Report Confidence

Environmental

- CIA Requirement
- Modified base score dimension

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



This is the version of CVSS used to score this flaw

This is the score for the issue.

Attack Vector - So the attack requires local access

Attack Complexity - The attack is difficult to execute

Privileges Required - It doesn’t need any local privileges

User Interaction - The attack requires user interaction

Scope - the vulnerable component impacts resources in components outside of its security scope.

C/I/A. - So the Confidentiality, Integrity, and Availability of files can be completely compromised.

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

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**

National Vulnerability Database - NVD

Issue not necessarily scored by technology-expert

Score does not take into account things like compiler switches, default hardening, nor tools like SELinux

No testing of reproducer against running environment

Generic score does not take into account different configurations or Operating Systems

Red Hat

Issue scored by Red Hat Product Security

Score accounts for build and configuration options that Red Hat uses

Score reflects actual testing and triage of the issue and specific products affected

Scoring is specific to configuration or Operating System

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

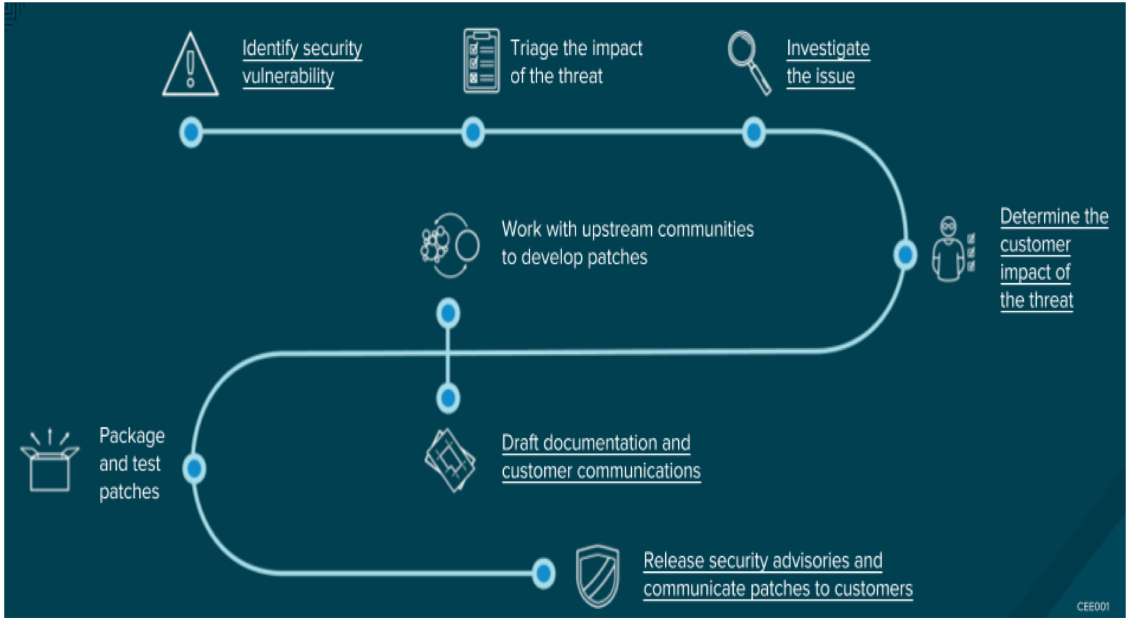
https://access.redhat.com/security/updates/classification/

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

CUSTOMER SECURITY AWARENESS EVENTS



Identify security vulnerability

Triage the impact of the threat

Investigate the issue

Determine the customer impact of the threat

Work with upstream communities to develop patches

Draft documentation and customer communications

Package and test patches

Release security advisories and communicate patches to customers

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

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**

POP QUIZ!!!

- How many of these vulnerabilities were rated CRITICAL?

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

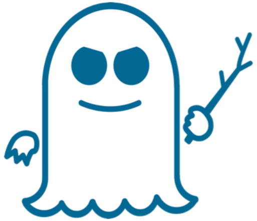
POP QUIZ!!!

CVE-2014-6271 Shellshock

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

POP QUIZ!!!

- Which of these branded vulnerabilities has the highest **CVSS risk?**



POP QUIZ!!!

CVSS != RISK

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.

QUESTIONS?