redhat.

Red Hat Product Security

Bringing Value to Customer Subscriptions

Transparency, objectivity, value.

SPEAKER INTRODUCTION

Chris Henderson
Sr. Program Manager, Product Security

- Over 20 years of Enterprise-class Architecture, Operations, Security experience
- 6 years with Red Hat
- RHCA
- Martial Arts enthusiast

Red Hat

PRODUCT SECURITY VISION

Red Hat Product Security's 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	Global Customer Success
Product Security	Global Support Services	CEE Strategic Services	Customer Content Services

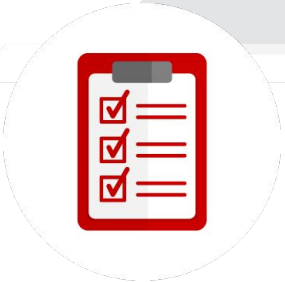
CUSTOMER PORTAL

Red Hat

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

Communicating the options for resolution and ensuring subscribers can act to protect themselves including using the CSAw process for significant issues

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

Reach out to secalert@redhat.com with any questions you may have

Red Hat

WHAT IS A SECURITY VULNERABILITY?

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.

There are many types of security vulnerabilities, among which the most concerning are:

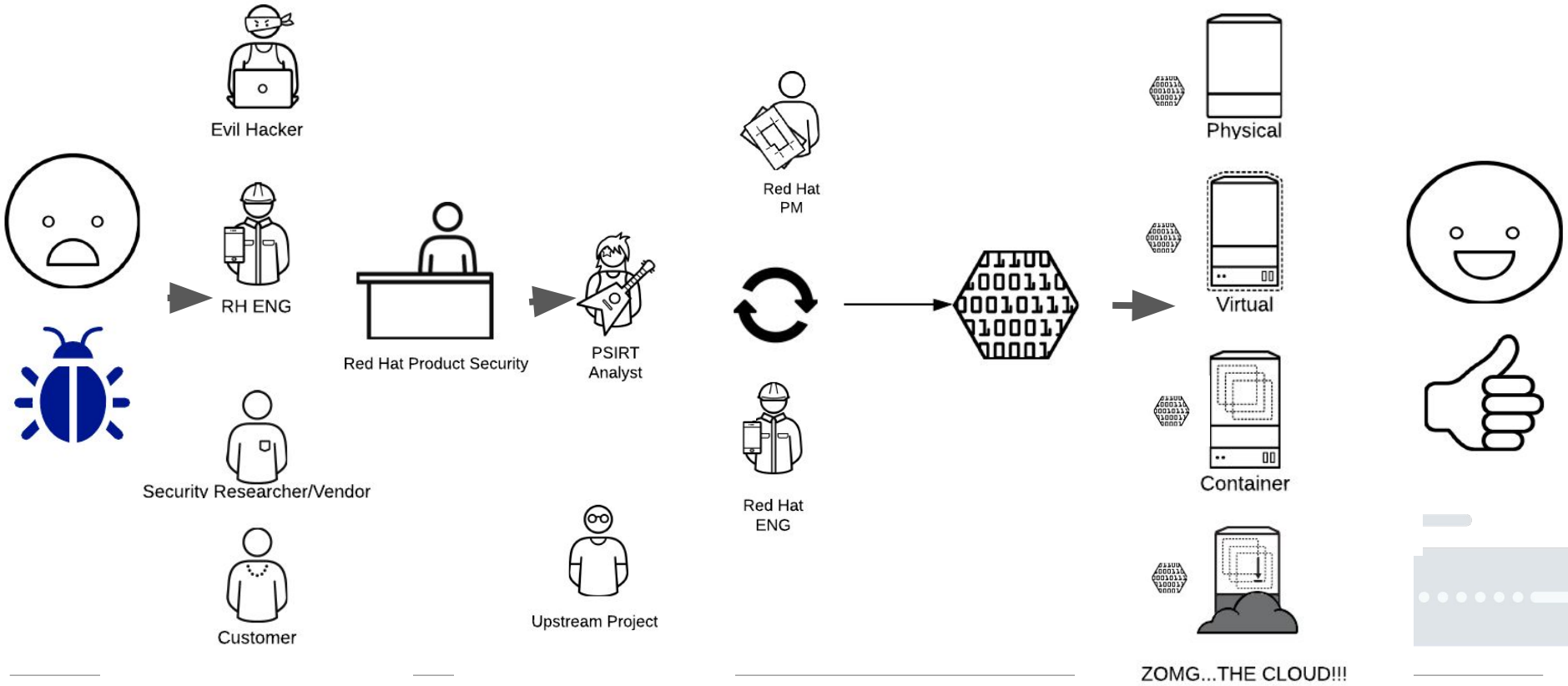
- Compromise of sensitive data (keys, financial information, customer information)
- Ability to execute arbitrary code on remote systems
- Denial of availability for mission-critical services

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, and
- the value of that system or asset

Red Hat

HOW A VULN REPORT TURNS INTO A PATCH



COMMON VULNERABILITIES AND EXPOSURES

Security Advisories | Red Hat CVE Database

Keyword GO

All | Low | Moderate | Important | Critical

	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-2017-42

CVE's all contain a brief description

A flaw in the memory manager of the Babel Fish could allow a malicious attacker to change output from the Babel Fish's translation

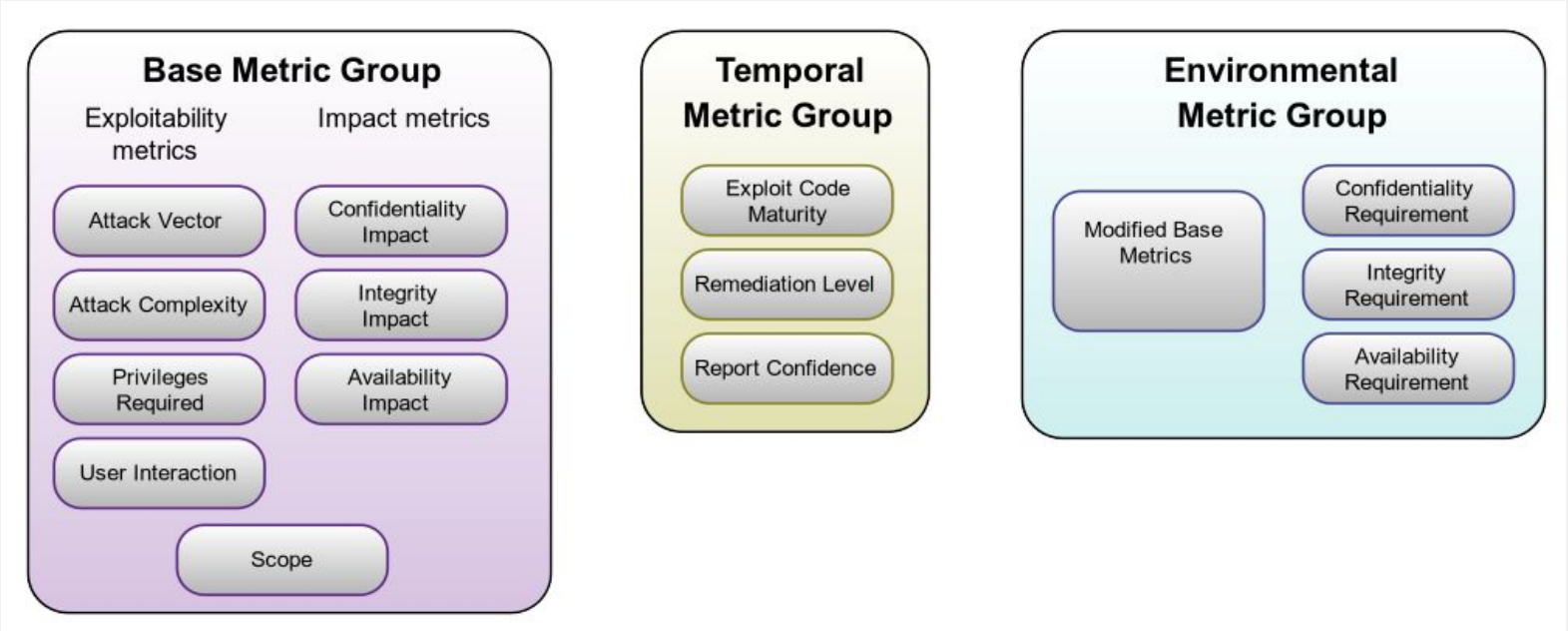
CVE's all include relevant references

Megadodo Industries Bug Tracker: 42
www.md.org.net.com/bz=42.htm

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

Red Hat

Common Vulnerability Scoring System (CVSS)



https://www.first.org/cvss/specification-document

WHAT DOES A CVSS SCORE LOOK LIKE?

CVSS:3.0- 9.8/AV:N/AC:L/PR:N/UI:N/S:U/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 comes across the network

Attack Complexity - The attack isn't very hard to execute

Privileges Required - It doesn't need any local privileges

User Interaction - The attack doesn't require any user interaction

Scope - The scope is unchanged, so the attack only works with the permissions of the service it has compromised.

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

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

Red Hat

CVSS != RISK

CVSS is just one data point in risk assessment

Other 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?

What risk factors do <u>you</u> need to consider?

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

https://www.redhat.com/en/blog/why-cvss-does-not-equal-risk-how-think-about-risk-your-environment

Red Hat

WHERE DO THE SCORES COME FROM?

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
- Only ONE score can exist (defers to package owner, then reporter, then MITRE reviewer)

Red Hat

- Issue scored by Red Hat Product Security
- Score accounts for build and configuration options that are Red Hat specific.
- Score reflects actual testing and triage of the issue and specific product versions affected
- Each product impacted could have different scores based off of default configuration

Red Hat

RED HAT SEVERITY RATINGS

CRITICAL	IMPORTANT	MODERATE	LOW
A remote unauthenticated user can execute arbitrary code Does not require user interaction i.e. Worms	Allows local users to gain privileges Unauthenticated remote users can view resources Authenticated remote users can execute arbitrary code	Are more difficult to exploit Are exploitable via an unlikely configuration	Unlikely circumstances for the exploit Are of minimal consequence

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

Red Hat

REPORTING SECURITY VULNERABILITIES

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

- notably for Red Hat products
- strongly recommended for upstream components in our products

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

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

IN 2018:

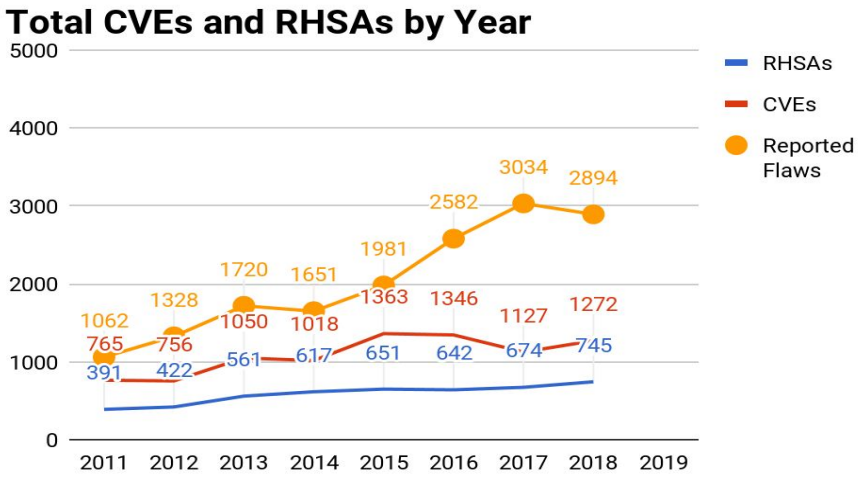
745 Red Hat SECURITY ADVISORIES

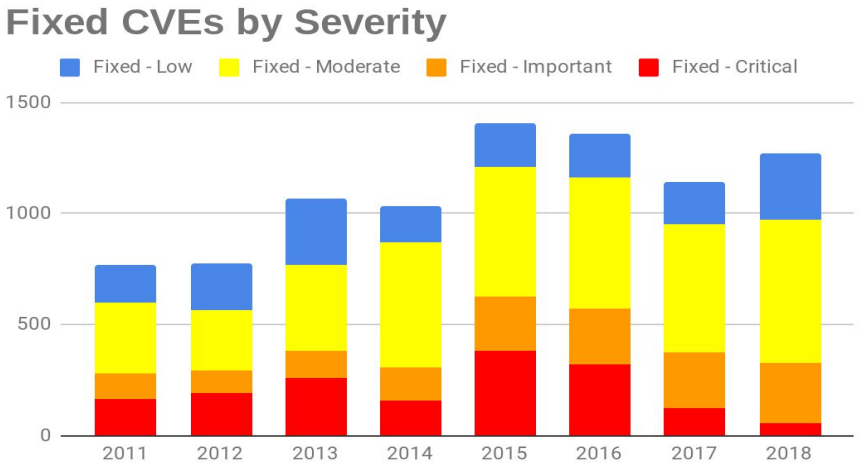
1,272 CVEs ADDRESSED

Source: 2018 Red Hat Product Security Risk Report, February 2019. red.ht/2018riskreport

VULNERABILITY METRICS

A snapshot of Red Hat Product Security response over the years





https://www.redhat.com/security/data/metrics/

Red Hat

Red Hat Product Security Resources - External

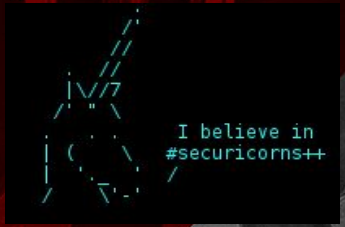
Red Hat Product Security Overview - https://access.redhat.com/security/overview/
RH Product Security Center - https://access.redhat.com/security
Red Hat Product Lifecycles - https://access.redhat.com/support/policy/update_policies/
Red Hat Security Severity Ratings - https://access.redhat.com/security/updates/classification/
Red Hat Errata Metrics - https://www.redhat.com/security/data/metrics/
Red Hat Security Vulnerability Data API - https://access.redhat.com/documentation/en-us/red_hat_security_data_api/1.0/html-single/red_hat_security_data_api/index
CSAw Vulnerability Pages - https://access.redhat.com/security/vulnerabilities/

Contact secalert@redhat.com

Red Hat

redhat.

THANK YOU



plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos