redhat

Red Hat Product Security

The annual Red Hat Product Security Risk Report

Transparency, objectivity, value.

SPEAKER INTRODUCTION

Chris Henderson
Sr. Program Manager, Product Security

- Over 20 years of Enterprise-class Architecture, Operations, Security experience
- 8 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 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

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.

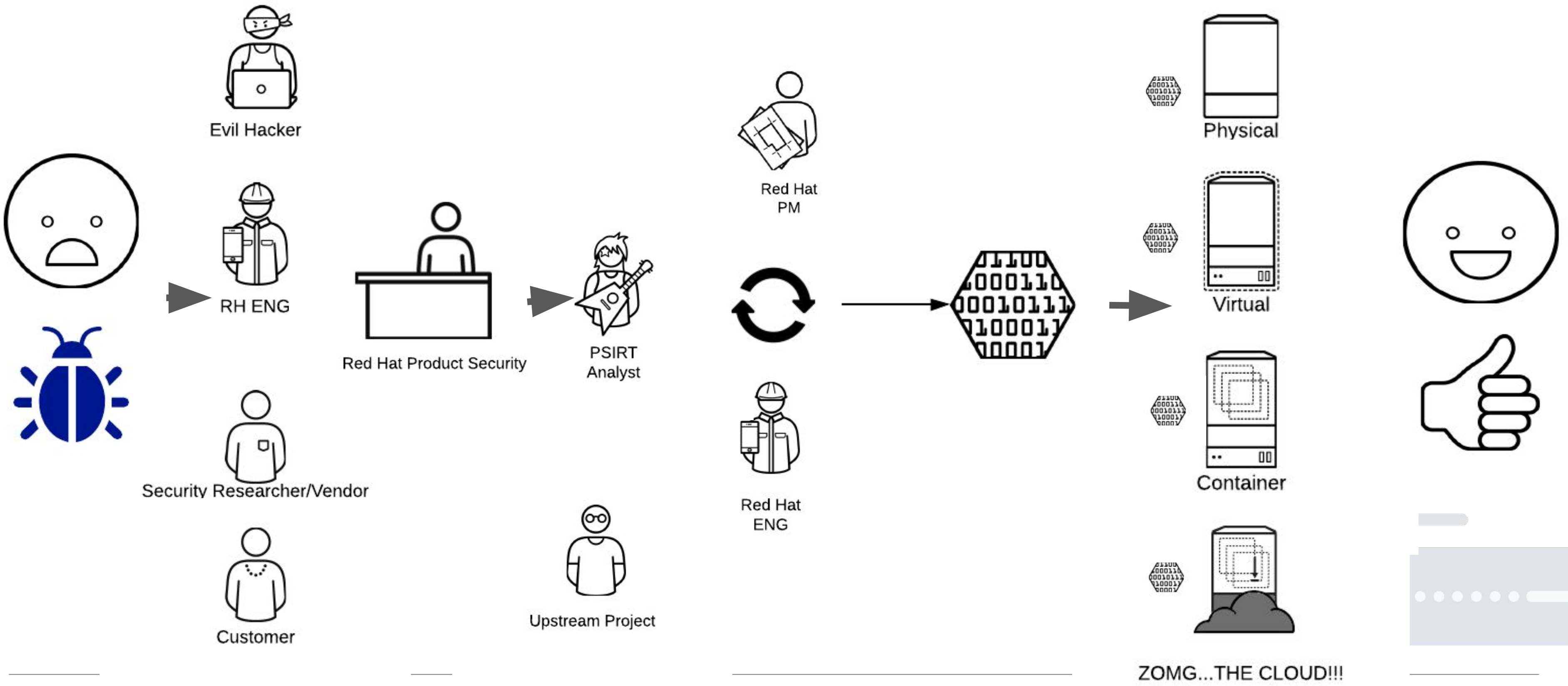
There are many types of security vulnerabilities, among which the most concerning are:

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

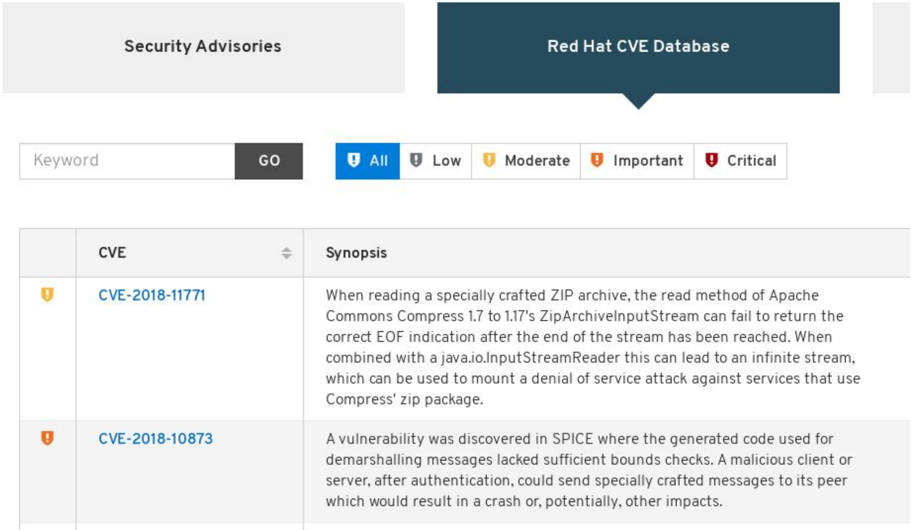
The severity of a vulnerability is determined by:

- 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

HOW A VULN REPORT TURNS INTO A PATCH



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

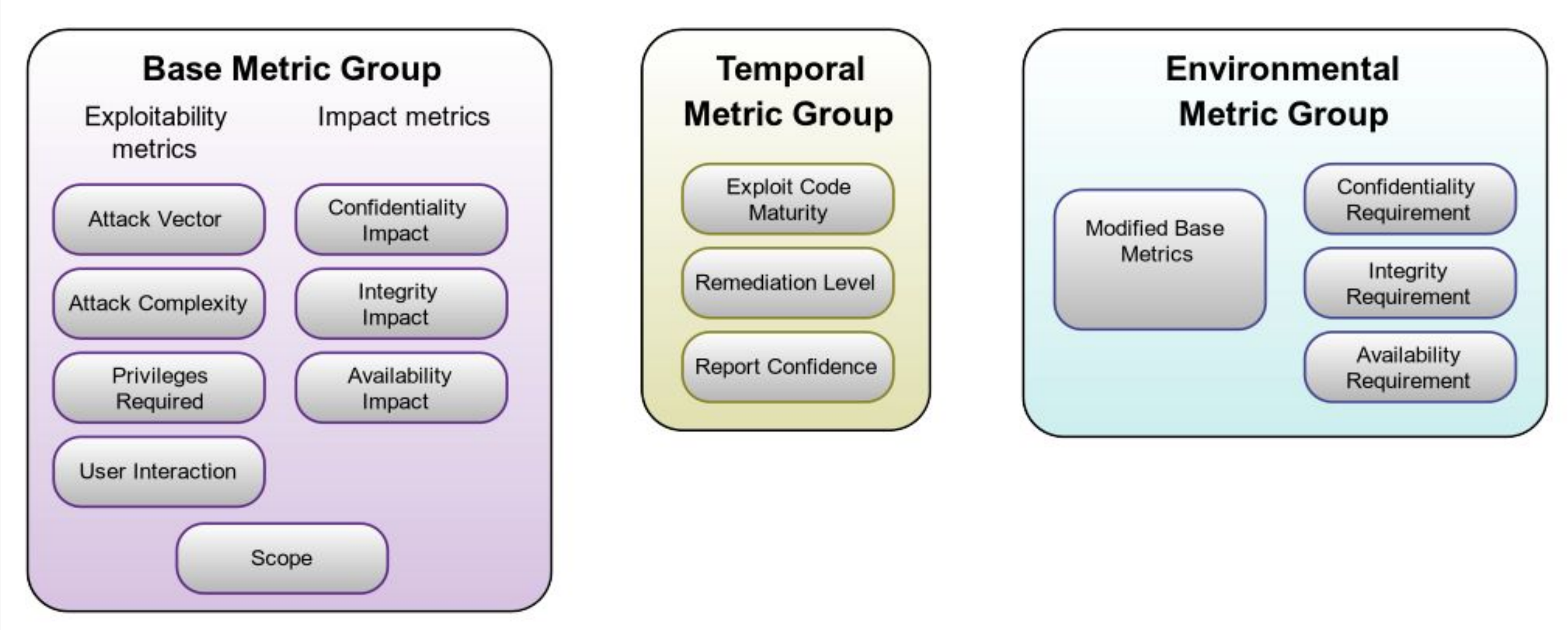
Common Weakness Enumeration - CWE

CWE is a common language used to describe the coding flaw that results in a vulnerability. Reviewing historic trends of weaknesses from a development team or project can help focus areas of analysis and training for future work.

Every CVE that impacts Red Hat Products also has a CWE identifier published alongside the CVSS score to help administrators and end-users better understand how a vulnerability arose and could be exploited.

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

Common Vulnerability Scoring System (CVSS)



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

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 you 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

WHERE DO THE SCORES COME FROM?

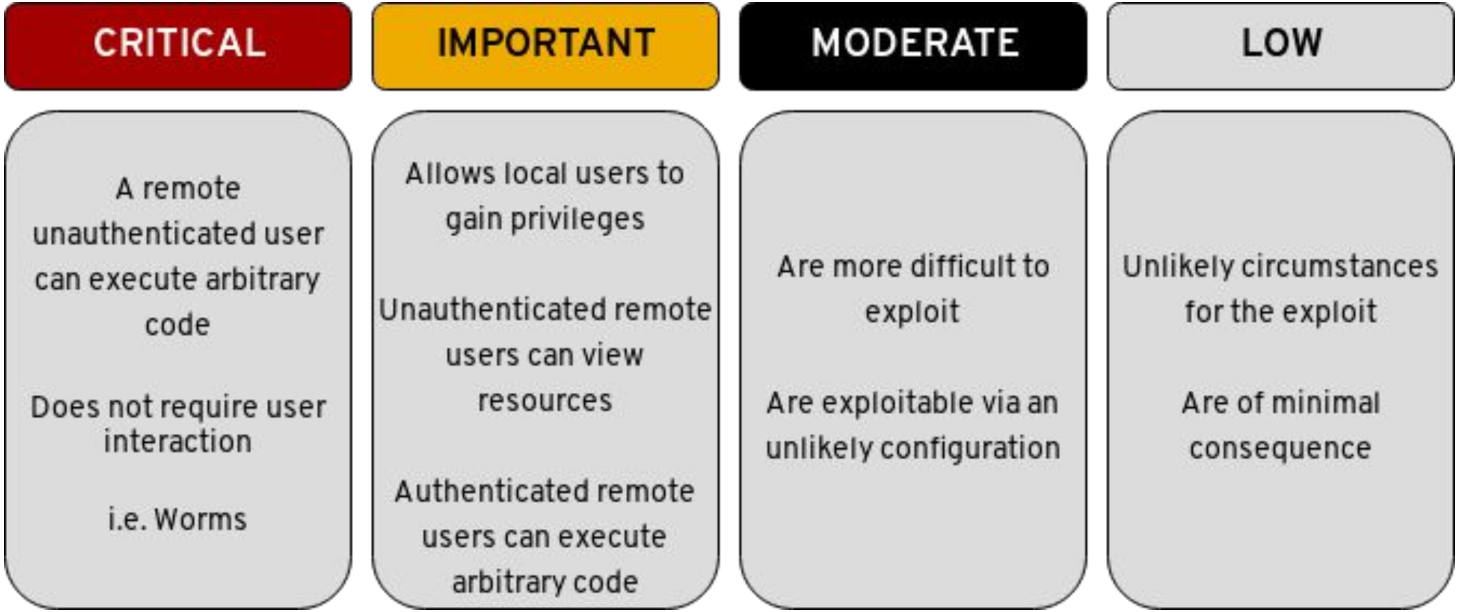
National Vulnerability Database - NVD

- 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 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/

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.

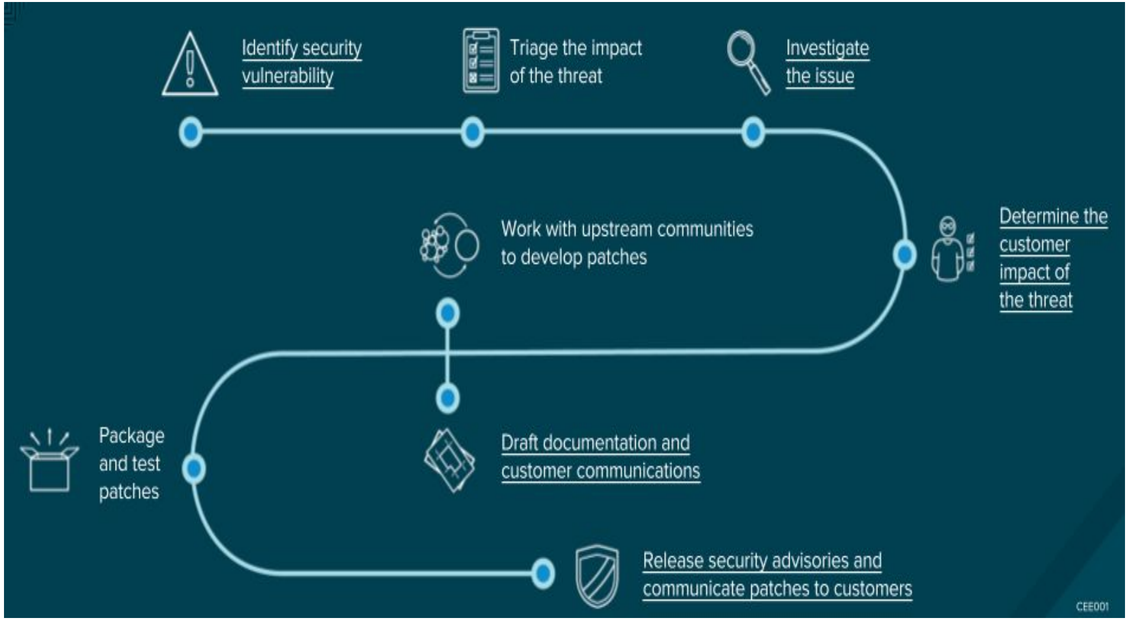
In the case of upstream projects, Product Security will help coordinate additional conversations and impose an embargo if required.

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
CEE001

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

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

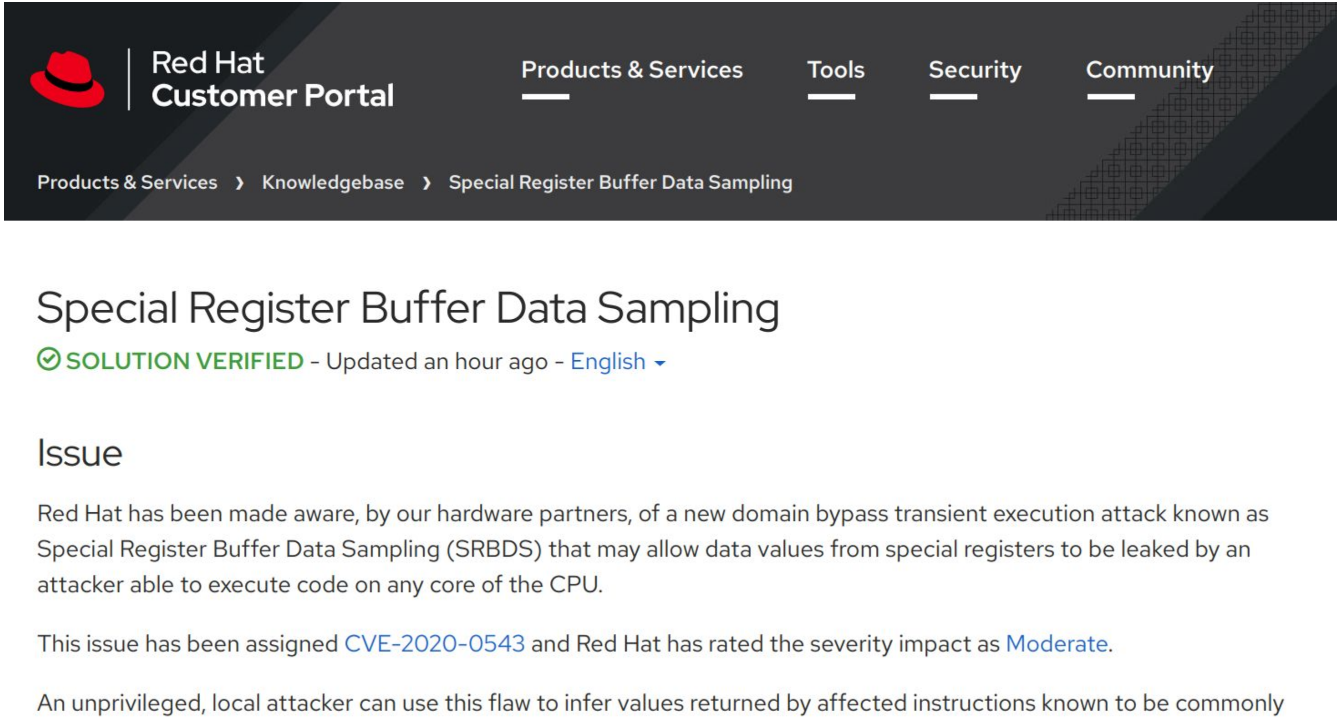
CSAW process helps ensure:

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

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

Red Hat

NEW VULNERABILITY


Red Hat
Customer Portal
Products & Services
Tools
Security
Community
Products & Services › Knowledgebase › Special Register Buffer Data Sampling

Special Register Buffer Data Sampling

✓ SOLUTION VERIFIED - Updated an hour ago - English ▾

Issue

Red Hat has been made aware, by our hardware partners, of a new domain bypass transient execution attack known as Special Register Buffer Data Sampling (SRBDS) that may allow data values from special registers to be leaked by an attacker able to execute code on any core of the CPU.

This issue has been assigned CVE-2020-0543 and Red Hat has rated the severity impact as Moderate.

An unprivileged, local attacker can use this flaw to infer values returned by affected instructions known to be commonly

https://access.redhat.com/solutions/5142691

OVAL

Open Vulnerability Assessment Language - OVAL

OVAL is a project that Red Hat Joined in 2002, and began releasing OVAL content for in 2006. It is a community-driven effort to help standardize the sharing of security content.

Tools like OpenSCAP ingest the OVAL feeds to help understand what security advisories are applicable to a scanned system. Many 3rd party vendors use this data too.

https://oval.mitre.org/about

Why OVAL is important

It helps form the linkage between the known vulnerability and the various versions of Red Hat products to which the fix has been ported.

- Identify the fixes and isolate them from any other changes
- Make sure the fixes do not introduce unwanted side effects
- Apply the fixes to our previously released versions
- Supply OVAL definitions that third-party vulnerability tools can use to determine the status of vulnerabilities (including backports).

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

Important OVAL changes

- 2006-2018 OVAL CVEs that had RHSA advisories published for RHEL
- 2019 OVAL was created for layered products that are based off of RPMs
- 2020 new feeds are being created that publish both fixed and unfixed CVEs applicable to RHEL and the RPM based layered products

https://www.redhat.com/security/data/oval/v2/
https://www.redhat.com/en/blog/evolving-oval/

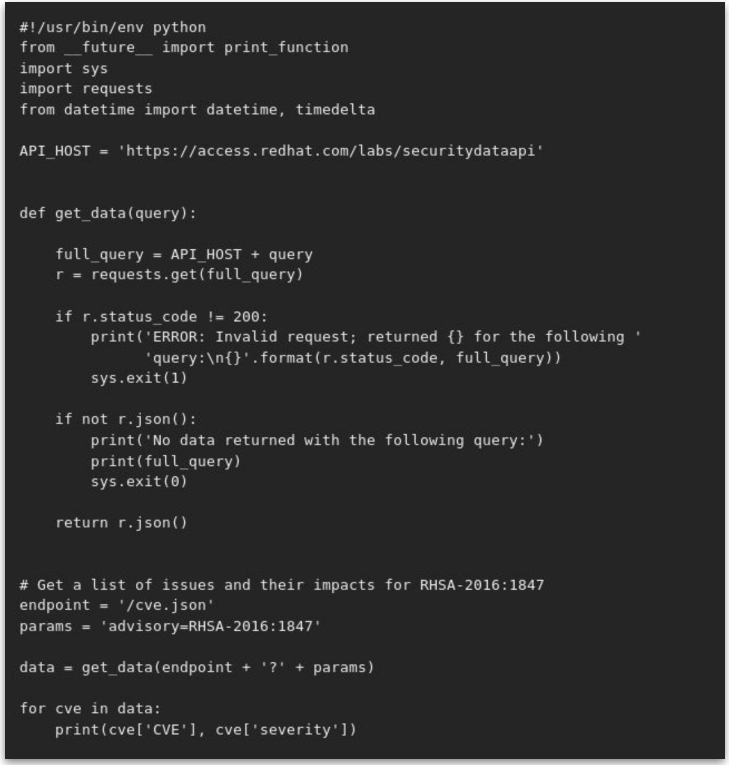
Security Data API

The data provided by the Security Data API is the same as what is found on the Security Data page:

- OVAL definitions
- Common Vulnerability Reporting Framework (CVRF)
- CVE data

All data is available in its native XML format or in a representative JSON format.

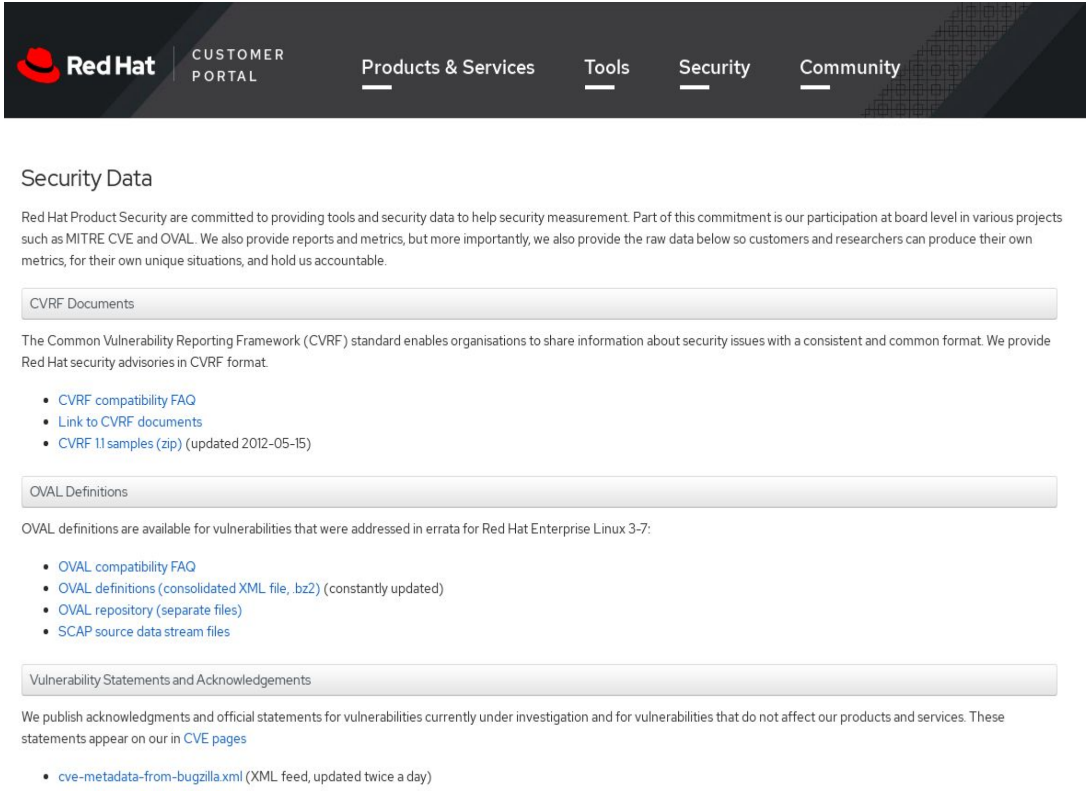
There is also a CLI tool available, rhsecapi



```
#!/usr/bin/env python
from __future__ import print_function
import sys
import requests
from datetime import datetime, timedelta

API_HOST = 'https://access.redhat.com/labs/securitydataapi'


def get_data(query):

    full_query = API_HOST + query
    r = requests.get(full_query)

    if r.status_code != 200:
        print('ERROR: Invalid request; returned {} for the following '
              'query:\n{}'.format(r.status_code, full_query))
        sys.exit(1)

    if not r.json():
        print('No data returned with the following query:')
        print(full_query)
        sys.exit(0)

    return r.json()


# Get a list of issues and their impacts for RHSA-2016:1847
endpoint = '/cve.json'
params = 'advisory=RHSA-2016:1847'

data = get_data(endpoint + '?' + params)

for cve in data:
    print(cve['CVE'], cve['severity'])
```

https://access.redhat.com/documentation/en-us/red_hat_security_data_api/1.0/html-single/red_hat_security_data_api/index

Security Data.... Your way



Security Data

Red Hat Product Security are committed to providing tools and security data to help security measurement. Part of this commitment is our participation at board level in various projects such as MITRE CVE and OVAL. We also provide reports and metrics, but more importantly, we also provide the raw data below so customers and researchers can produce their own metrics, for their own unique situations, and hold us accountable.

CVRF Documents

The Common Vulnerability Reporting Framework (CVRF) standard enables organisations to share information about security issues with a consistent and common format. We provide Red Hat security advisories in CVRF format.

- CVRF compatibility FAQ
- Link to CVRF documents
- CVRF 1.1 samples (zip) (updated 2012-05-15)

OVAL Definitions

OVAL definitions are available for vulnerabilities that were addressed in errata for Red Hat Enterprise Linux 3-7:

- OVAL compatibility FAQ
- OVAL definitions (consolidated XML file, .bz2) (constantly updated)
- OVAL repository (separate files)
- SCAP source data stream files

Vulnerability Statements and Acknowledgements

We publish acknowledgments and official statements for vulnerabilities currently under investigation and for vulnerabilities that do not affect our products and services. These statements appear on our in CVE pages

- cve-metadata-from-bugzilla.xml (XML feed, updated twice a day)

Whether you're a command-line "do it yourself'er", an API-coder, or you enjoy a pleasing Webified User Interface, Red Hat Product Security offers numerous paths for you to get the information you NEED about security vulnerabilities.

BY THE NUMBERS

2019 AT A GLANCE

- 2,714 security issues were reported to Red Hat Product Security (slightly down from 2018)
- 1,313 CVEs were addressed throughout 2019, a 3.2% increase from 2018
- 968 Red Hat Security Advisories were issued, a record increase over previous years
- 40 Critical advisories addressed 27 Critical vulnerabilities
- 41% of Critical issues were addressed within 1 business day
- 85% of Critical issues were addressed within 1 week

https://www.redhat.com/en/resources/product-security-risk-report-overview

VULNERABILITY METRICS

A snapshot of Red Hat Product Security response over the years

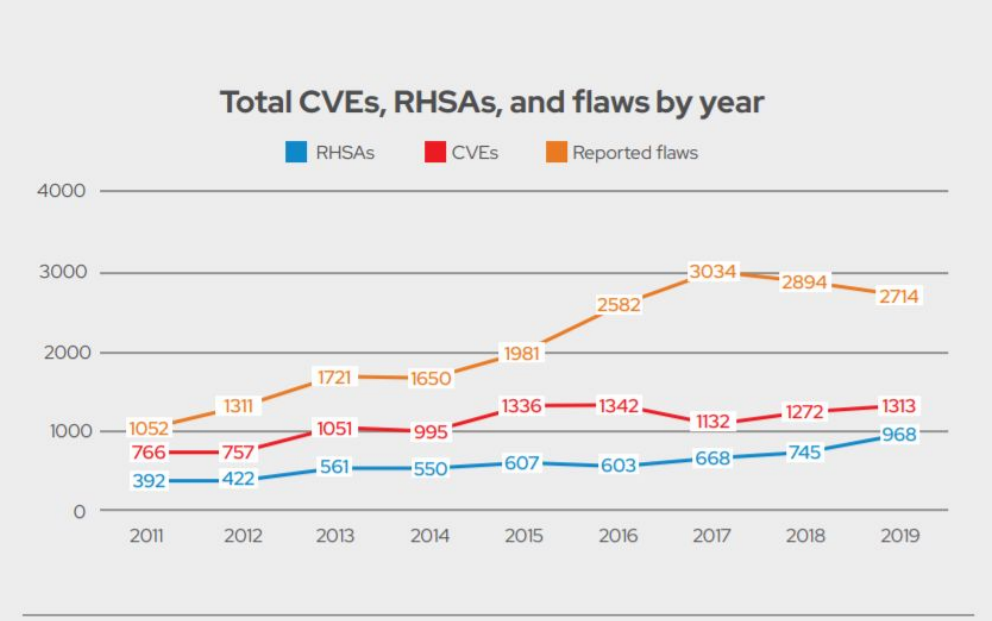
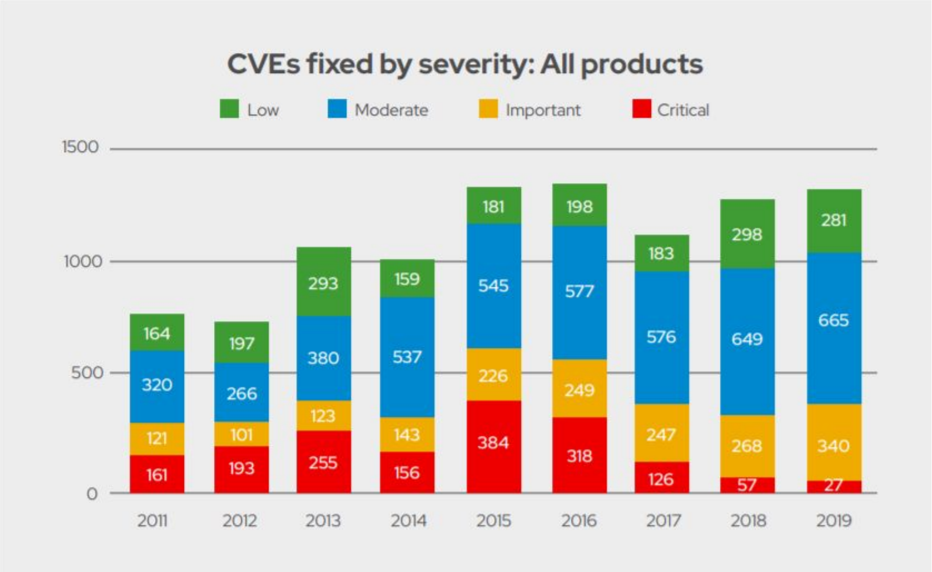


Figure 1. Total CVEs, RHSAs, and flaws

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

VULNERABILITY METRICS

A snapshot of Red Hat Product Security response over the years



CVEs fixed by severity: All products

Figure 2. CVEs fixed by severity

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

VULNERABILITY METRICS

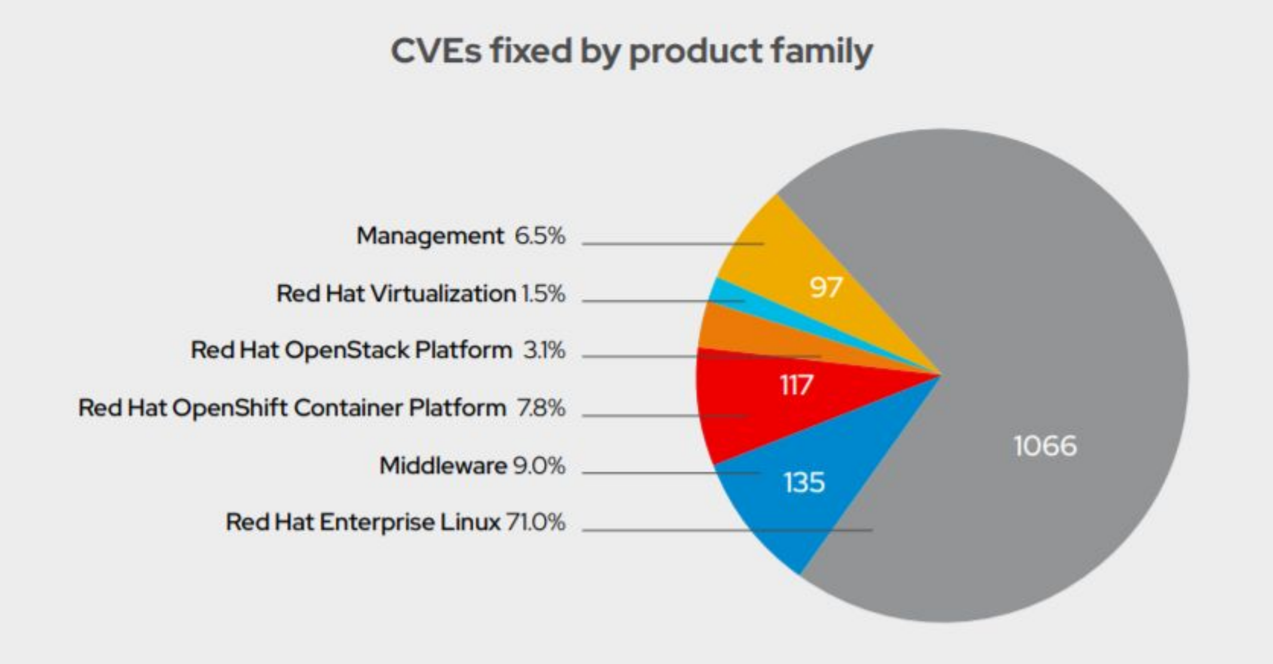


Figure 3. CVEs by product or product family

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

Red Hat Product Security Resources

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
Vulnerability Response Pages - https://access.redhat.com/security/vulnerabilities/

Contact secalert@redhat.com

THANK YOU

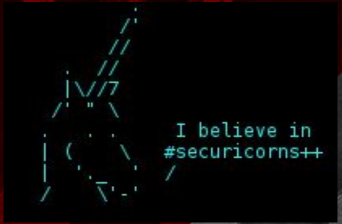
plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos



```
I believe in
#securicorns++
```