Vulnerability Management and Compliance

International Common Criteria Conference, Qatar, 2024

Vincent Danen

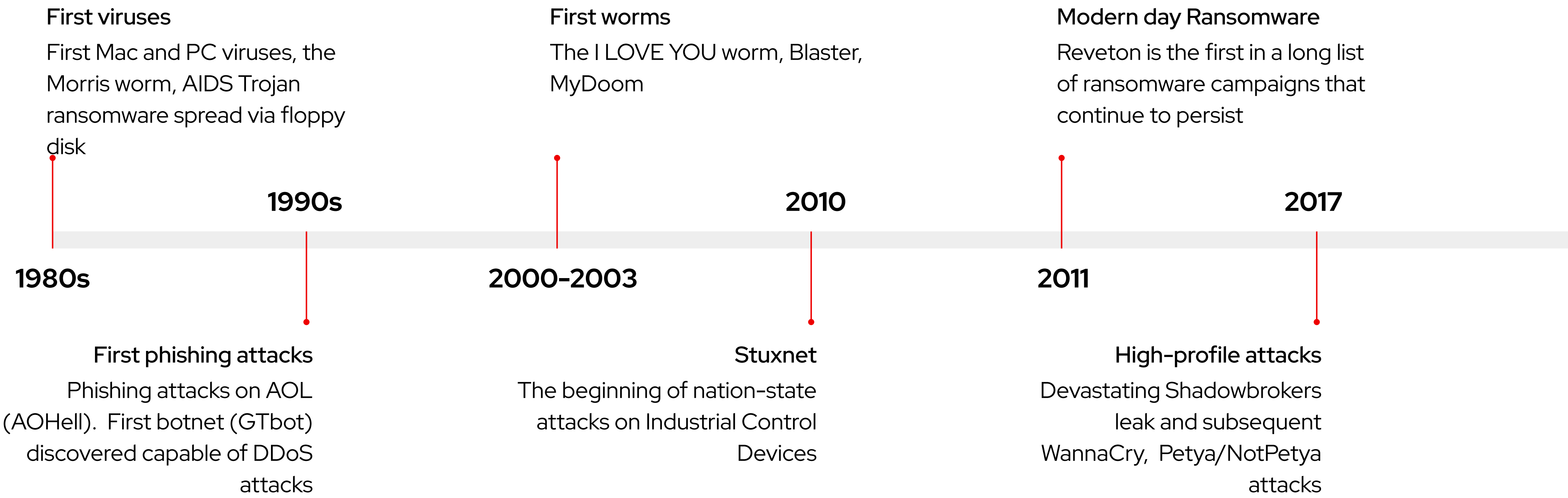
Vice President, Red Hat Product Security

Red Hat

Security is top of mind.

From vulnerabilities and breaches to post-quantum and AI, security is being discussed, especially as it relates to open source.

Evolution of Cybercrime



1980s

First viruses

First Mac and PC viruses, the Morris worm, AIDS Trojan ransomware spread via floppy disk

1990s

First phishing attacks

Phishing attacks on AOL (AOHell). First botnet (GTbot) discovered capable of DDoS attacks

2000-2003

First worms

The I LOVE YOU worm, Blaster, MyDoom

2010

Stuxnet

The beginning of nation-state attacks on Industrial Control Devices

2011

Modern day Ransomware

Reveton is the first in a long list of ransomware campaigns that continue to persist

2017

High-profile attacks

Devastating Shadowbrokers leak and subsequent WannaCry, Petya/NotPetya attacks

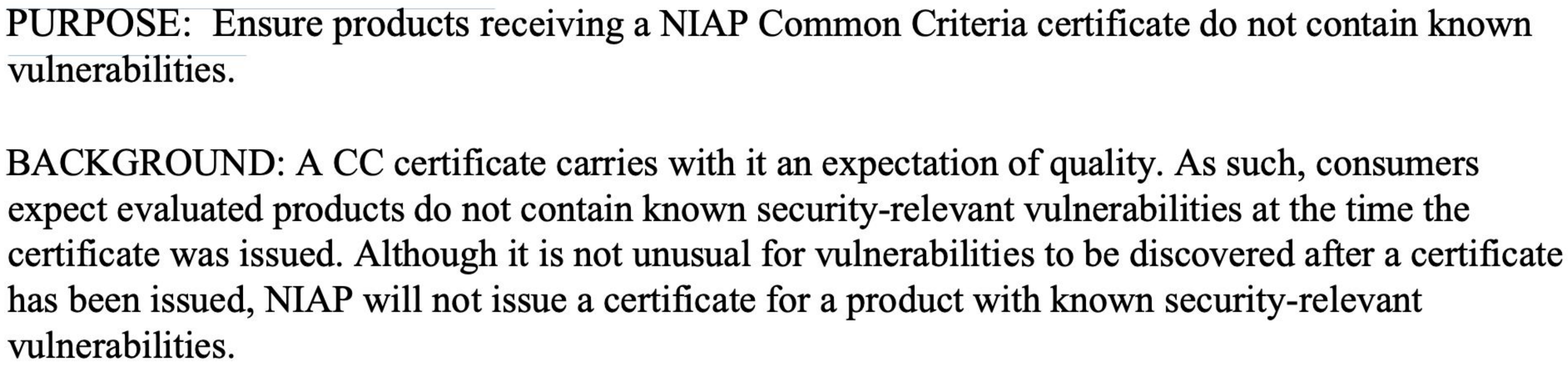
Source: Fortinet, A Brief History of The Evolution of Malware
https://www.fortinet.com/blog/threat-research/evolution-of-malware

0

KNOWN VULNERABILITIES

Common Criteria

All known vulnerabilities at certification



PURPOSE: Ensure products receiving a NIAP Common Criteria certificate do not contain known vulnerabilities.

BACKGROUND: A CC certificate carries with it an expectation of quality. As such, consumers expect evaluated products do not contain known security-relevant vulnerabilities at the time the certificate was issued. Although it is not unusual for vulnerabilities to be discovered after a certificate has been issued, NIAP will not issue a certificate for a product with known security-relevant vulnerabilities.

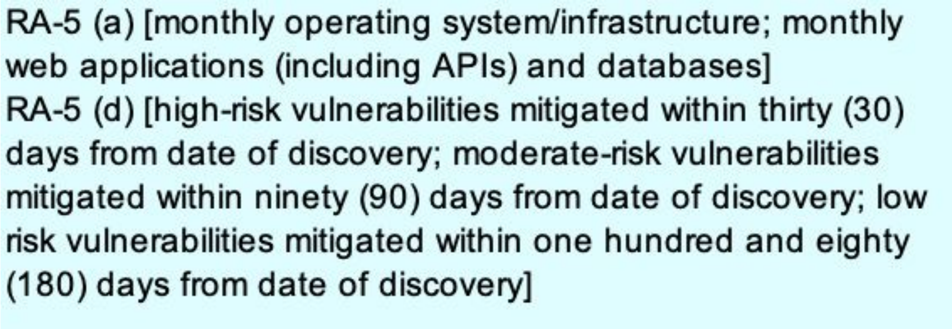
Effects of Vulnerabilities in Evaluated Products
https://www.niap-ccevs.org/static_html/policies/policy-ltr-17-update2.pdf

Not only Common Criteria

FedRAMP

All known vulnerabilities

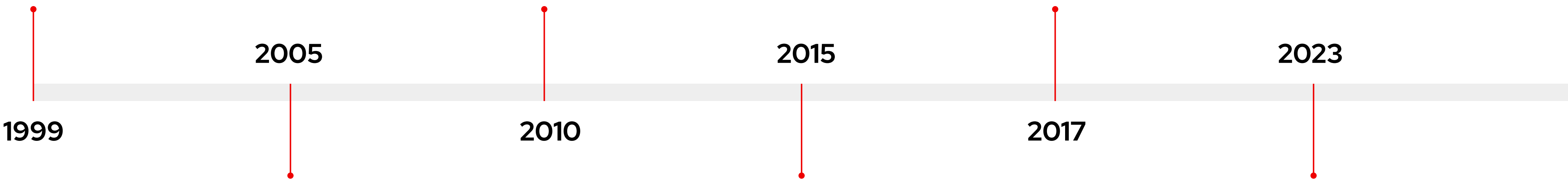
↓



RA-5 (a) [monthly operating system/infrastructure; monthly web applications (including APIs) and databases]
RA-5 (d) [high-risk vulnerabilities mitigated within thirty (30) days from date of discovery; moderate-risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery]

FedRAMP Security Controls Baseline
https://www.fedramp.gov/documents-templates/

Vulnerabilities continue to increase



1999
First year of CVE
894

2005
452% increase over 6 years
4932

2010
Steady state
4639

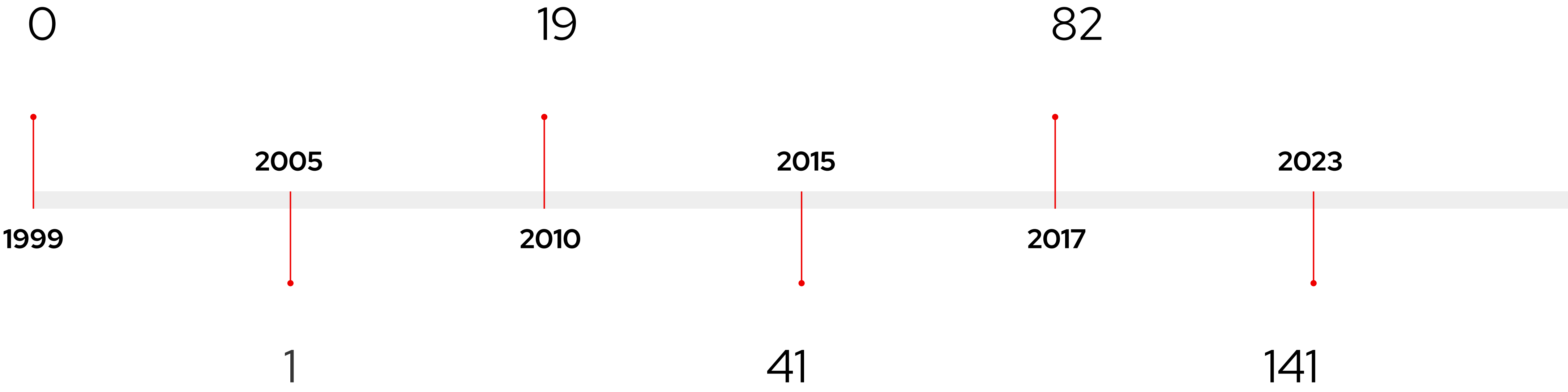
2015
40% increase over 5 years
6494

2017
125% increase over 2 years!
14643

2023
50% increase over 6 years
29065

Source: CVE Details
https://www.cvedetails.com/

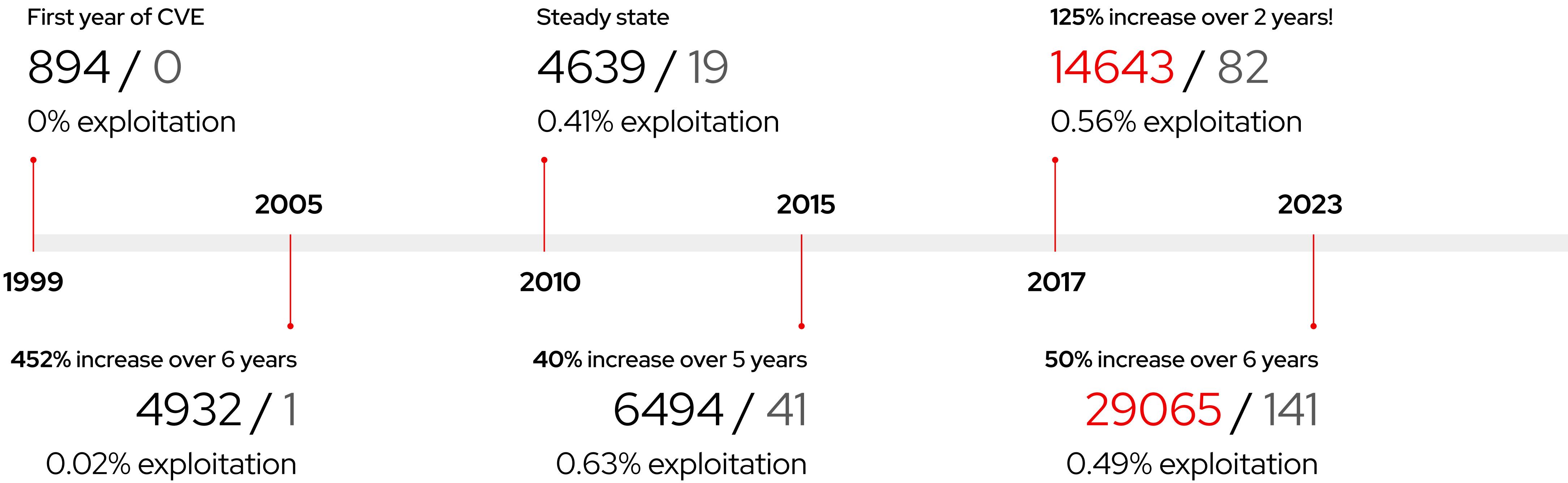
Exploitation continues to increase



1999	0
2005	1
2010	19
2015	41
2017	82
2023	141

Source: CISA Known Exploited Vulnerabilities Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Vulnerabilities vs Exploitation



1999

First year of CVE

894 / 0

0% exploitation

2005

452% increase over 6 years

4932 / 1

0.02% exploitation

2010

Steady state

4639 / 19

0.41% exploitation

2015

40% increase over 5 years

6494 / 41

0.63% exploitation

2017

125% increase over 2 years!

14643 / 82

0.56% exploitation

2023

50% increase over 6 years

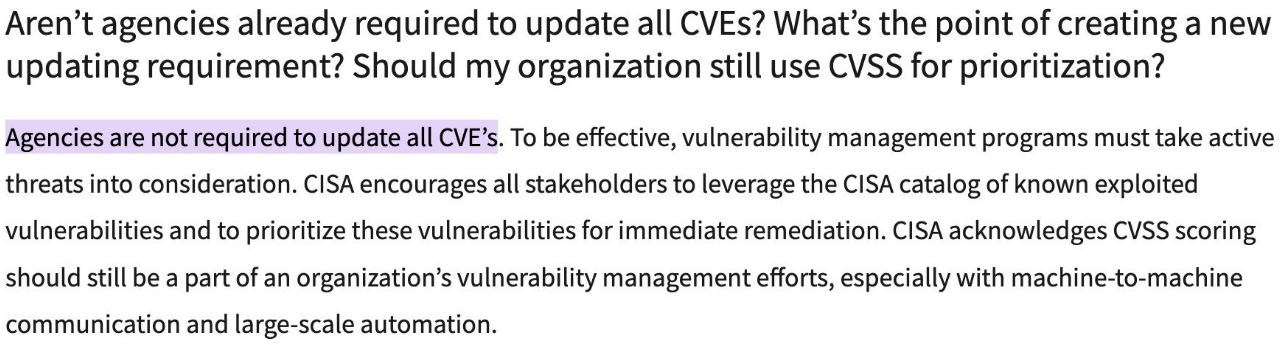
29065 / 141

0.49% exploitation

Source: CVE Details
https://www.cvedetails.com/

Not only Common Criteria

Only Critical, Important and
exploited vulnerabilities



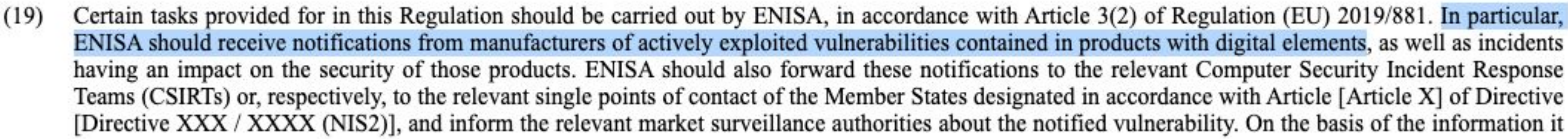
Aren’t agencies already required to update all CVEs? What’s the point of creating a new updating requirement? Should my organization still use CVSS for prioritization?

Agencies are not required to update all CVE’s. To be effective, vulnerability management programs must take active threats into consideration. CISA encourages all stakeholders to leverage the CISA catalog of known exploited vulnerabilities and to prioritize these vulnerabilities for immediate remediation. CISA acknowledges CVSS scoring should still be a part of an organization’s vulnerability management efforts, especially with machine-to-machine communication and large-scale automation.

CISA BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities
https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities

Not only Common Criteria

Notification of actively exploited vulnerabilities (and patch)



(19) Certain tasks provided for in this Regulation should be carried out by ENISA, in accordance with Article 3(2) of Regulation (EU) 2019/881. In particular, ENISA should receive notifications from manufacturers of actively exploited vulnerabilities contained in products with digital elements, as well as incidents having an impact on the security of those products. ENISA should also forward these notifications to the relevant Computer Security Incident Response Teams (CSIRTs) or, respectively, to the relevant single points of contact of the Member States designated in accordance with Article [Article X] of Directive [Directive XXX / XXXX (NIS2)], and inform the relevant market surveillance authorities about the notified vulnerability. On the basis of the information it

Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454

Severity impact and CVSS

CRITICAL

- A remote unauthenticated user can execute arbitrary code
- Does not require user interaction
- i.e. Worms

IMPORTANT

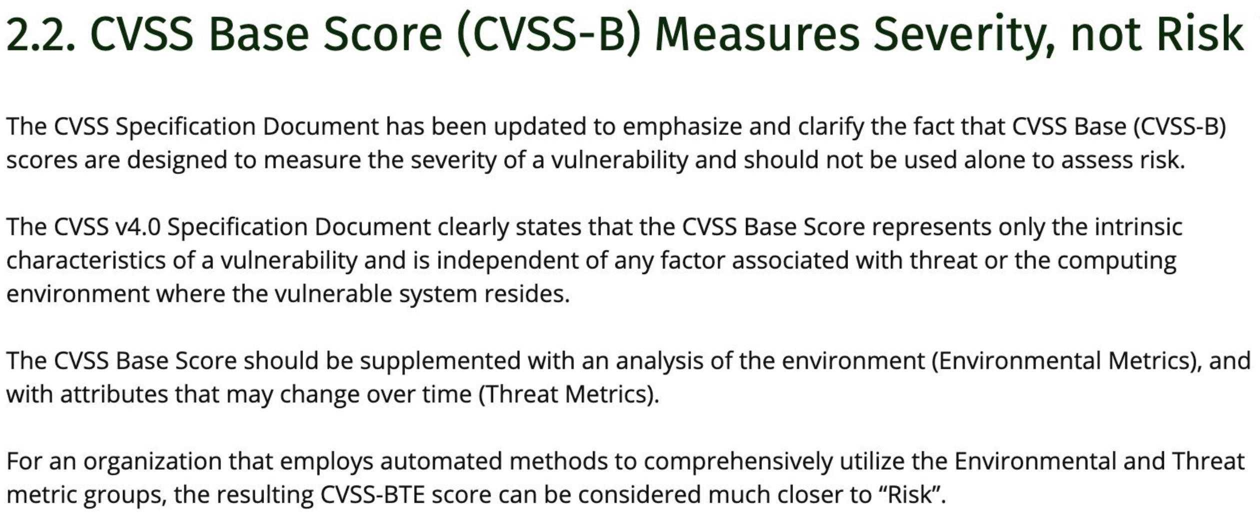
- Allows local users to gain privileges
- Unauthenticated remote users can view resources
- Authenticated remote users can execute arbitrary code

MODERATE

- Vulnerabilities are more difficult to exploit
- Are exploitable via an unlikely configuration

LOW

- Unlikely circumstances required to exploit
- Impact is of minimal consequence



2.2. CVSS Base Score (CVSS-B) Measures Severity, not Risk

The CVSS Specification Document has been updated to emphasize and clarify the fact that CVSS Base (CVSS-B) scores are designed to measure the severity of a vulnerability and should not be used alone to assess risk.

The CVSS v4.0 Specification Document clearly states that the CVSS Base Score represents only the intrinsic characteristics of a vulnerability and is independent of any factor associated with threat or the computing environment where the vulnerable system resides.

The CVSS Base Score should be supplemented with an analysis of the environment (Environmental Metrics), and with attributes that may change over time (Threat Metrics).

For an organization that employs automated methods to comprehensively utilize the Environmental and Threat metric groups, the resulting CVSS-BTE score can be considered much closer to "Risk".

Source: FIRST CVSS v4.0 user guide
https://www.first.org/cvss/v4.0/user-guide

Risk by the numbers

Critical	Important	Moderate	Low	All
12 discovered 1 known exploited	336 discovered 15 known exploited	1,047 discovered 3 known exploited	275 discovered 1 known exploited	1,670* discovered 20 known exploited
8.3%	4.5%	0.3%	0.4%	1.2%

Source:Red Hat Product Security risk report 2023
https://www.redhat.com/en/resources/product-security-risk-report-2023
* 1670 vulnerabilities in 2023 for the entire Red Hat portfolio of products

0

“KNOWN” VULNERABILITIES

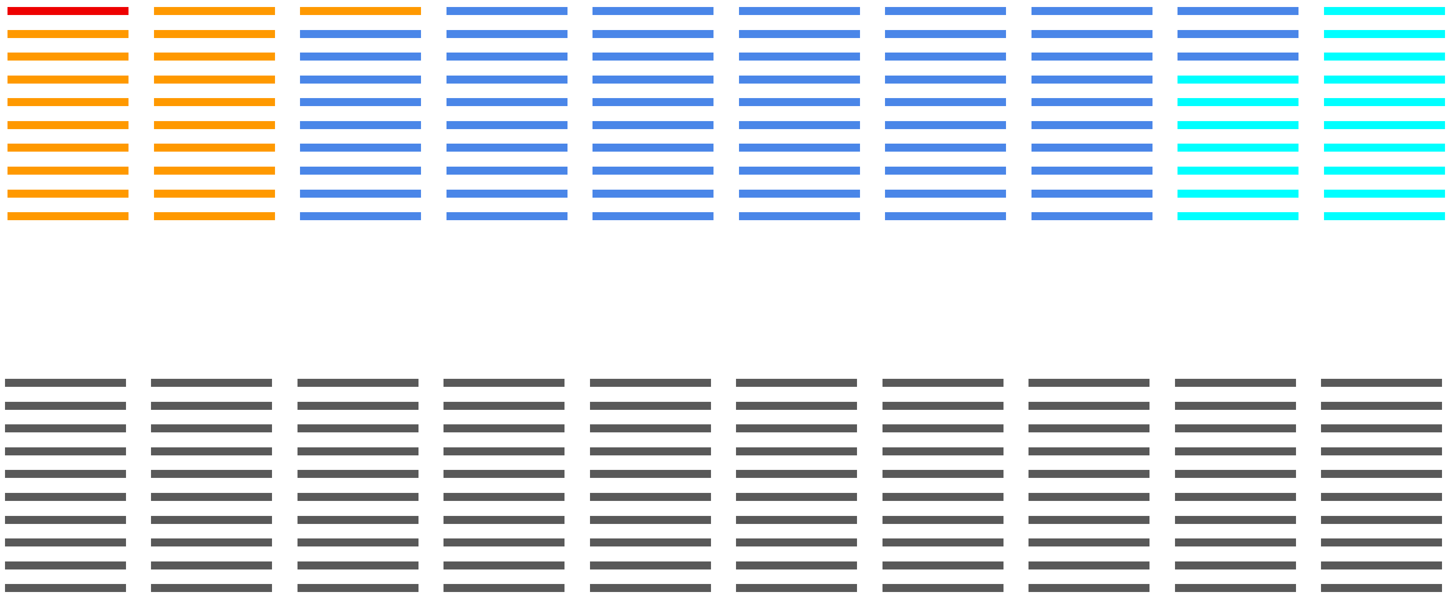
Risk by the numbers

Critical	Important	Moderate	Low	All
100 reported	**890** reported	**32** reported	**16** reported	**1,281** total reported
2 reported exploited	**22** reported exploited	**3** reported exploited	**0** reported exploited	**1,038** with ratings
				27 known exploited
2%	2.5%	9.4%	0%	2.6%

Source: Unnamed major proprietary vendor that actually publishes really good security information on publicly known vulnerabilities

Vendor A		Vendor B
CRITICAL	Remote unauthenticated arbitrary code execution User interaction not required (Worms)	CRITICAL
	Allows local users to elevate privileges Unauthenticated remote users can view resources Authenticated remote arbitrary code execution	
	Vulnerabilities are more difficult to exploit Are exploitable via an unlikely configuration	
LOW	Unlikely circumstances required to exploit Impact is of minimal consequence	LOW

Severity Weights



Red Hat

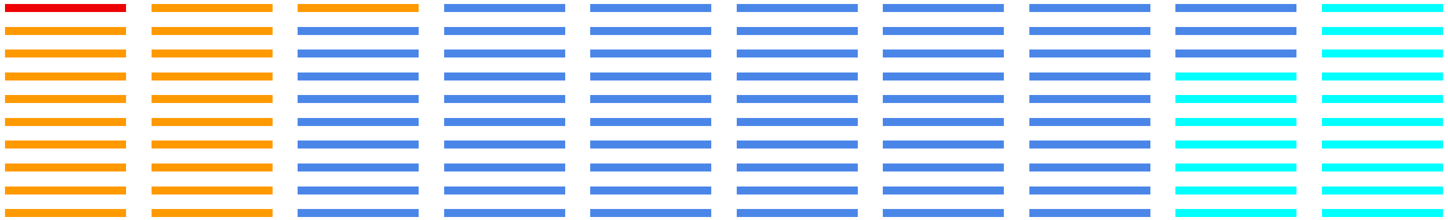
.7% Critical

20.1% Important

62.7% Moderate

16.5% Low

Severity Weights



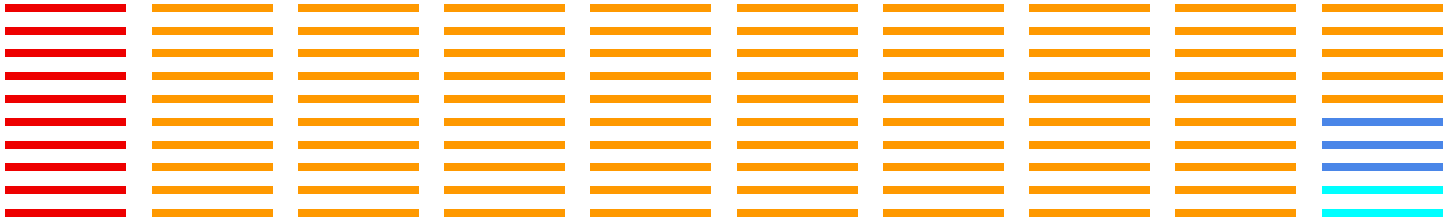
Red Hat

.7% Critical

20.1% Important

62.7% Moderate

16.5% Low



Proprietary

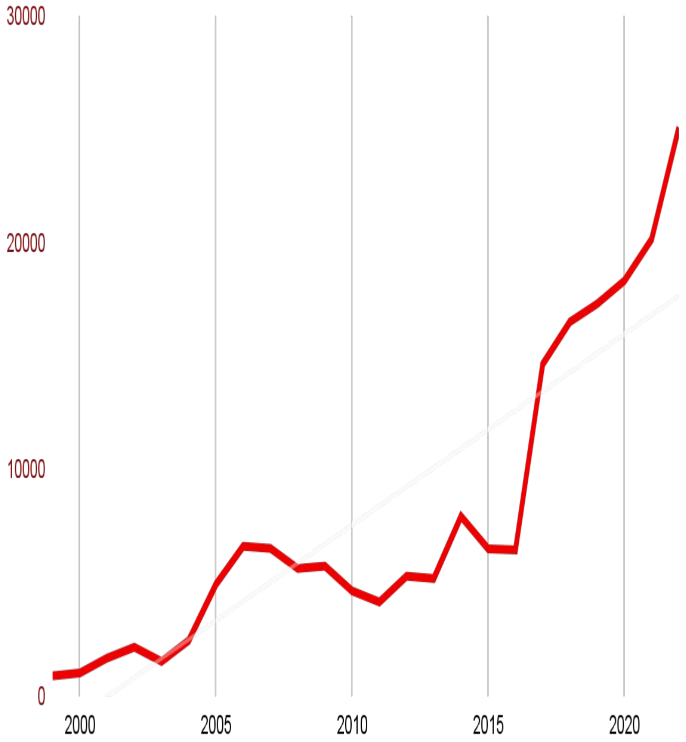
9.6% Critical

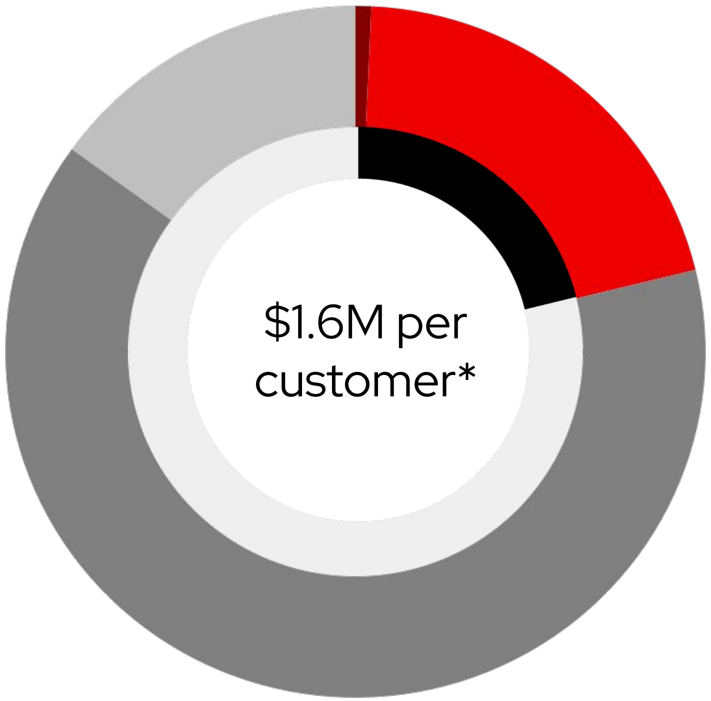
85.7% Important

3% Moderate

1.5% Low

Cost to avoid (2023)





$336,000
Fix all Important
(15 exploited,
$22,400 each)

$12,000
Fix all Critical
(1 exploited,
$12,000 each)

$348,000
Fix all risky
(16 exploited,
$21,750 each)

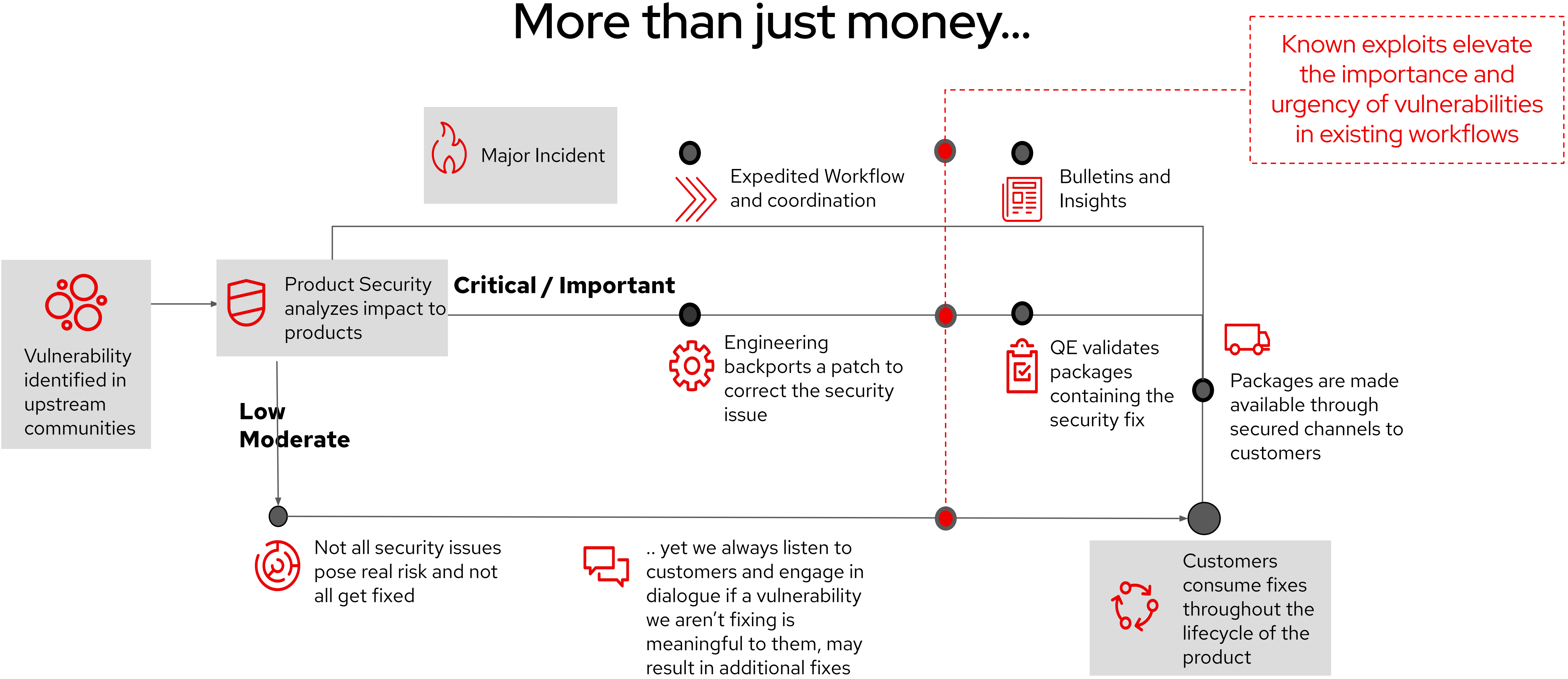
$1,047,000
Fix all Moderate
(3 exploited,
$349,000 each)

$247,000
Fix all Low
(1 exploited,
$247,000 each 🔥)

$1,294,000
Fix all not risky
(4 exploited,
$323,500 each)

* Using the assumption that every vulnerability costs a customer $1000 to fix (test and deploy).

More than just money...



Known exploits elevate the importance and urgency of vulnerabilities in existing workflows

Major Incident

Expedited Workflow and coordination

Bulletins and Insights

Vulnerability identified in upstream communities

Product Security analyzes impact to products

Critical / Important

Engineering backports a patch to correct the security issue

QE validates packages containing the security fix

Packages are made available through secured channels to customers

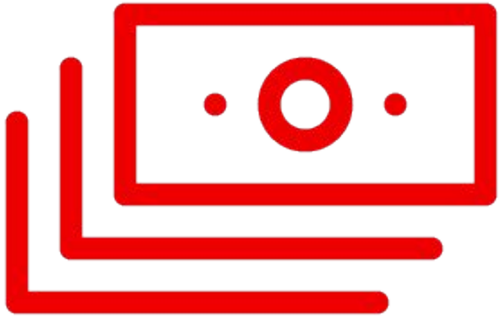
Low
Moderate

Not all security issues pose real risk and not all get fixed

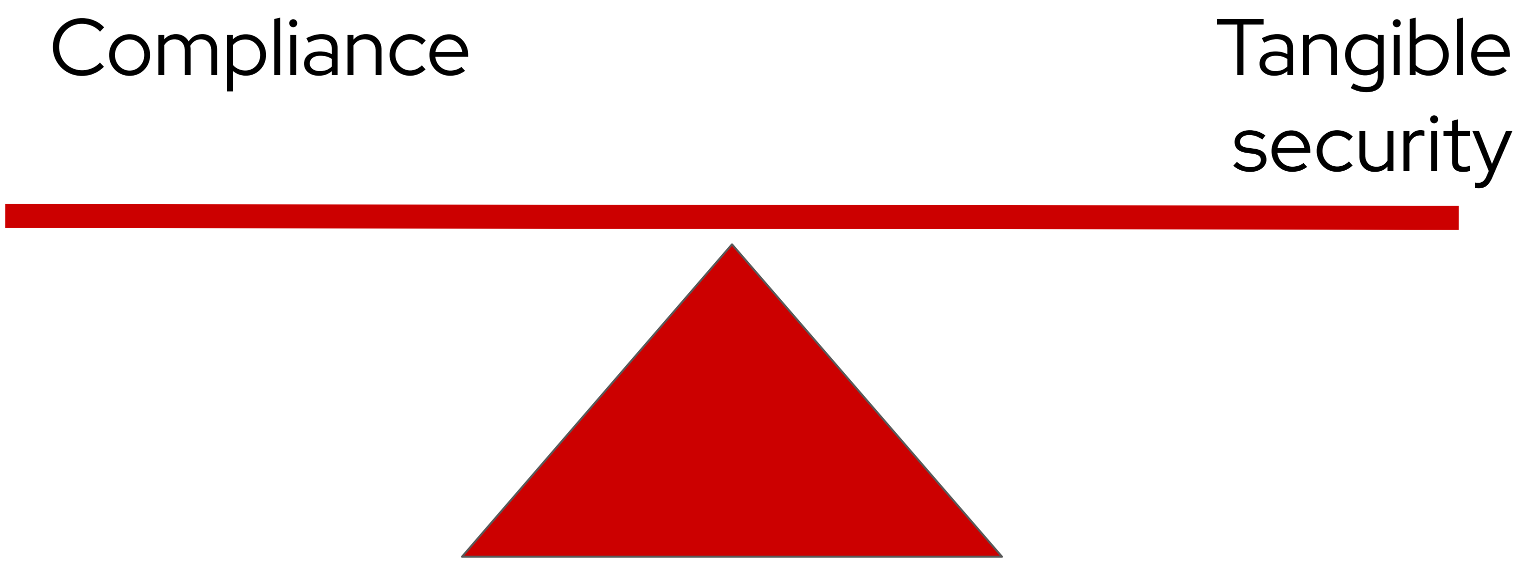
.. yet we always listen to customers and engage in dialogue if a vulnerability we aren't fixing is meaningful to them, may result in additional fixes

Customers consume fixes throughout the lifecycle of the product

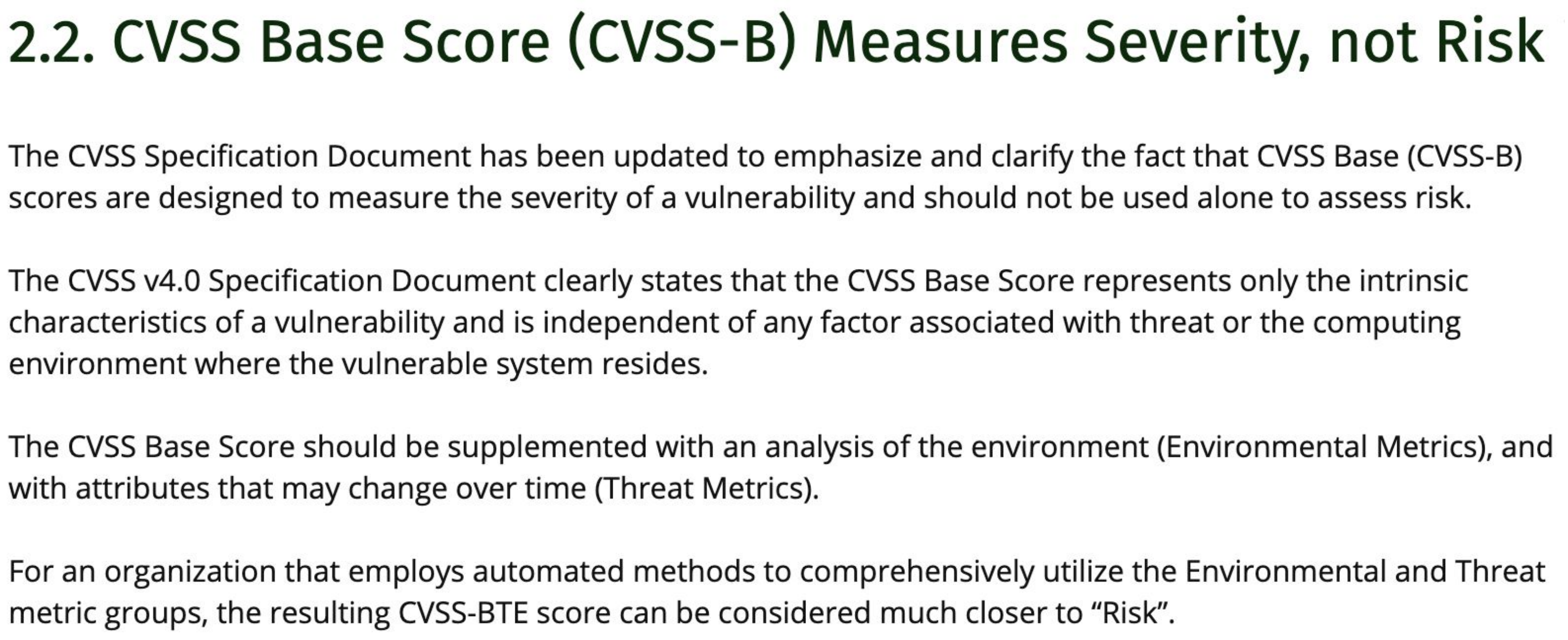
More than just money...



A little bit of controversy?



Common Vulnerability Scoring System



2.2. CVSS Base Score (CVSS-B) Measures Severity, not Risk

The CVSS Specification Document has been updated to emphasize and clarify the fact that CVSS Base (CVSS-B) scores are designed to measure the severity of a vulnerability and should not be used alone to assess risk.

The CVSS v4.0 Specification Document clearly states that the CVSS Base Score represents only the intrinsic characteristics of a vulnerability and is independent of any factor associated with threat or the computing environment where the vulnerable system resides.

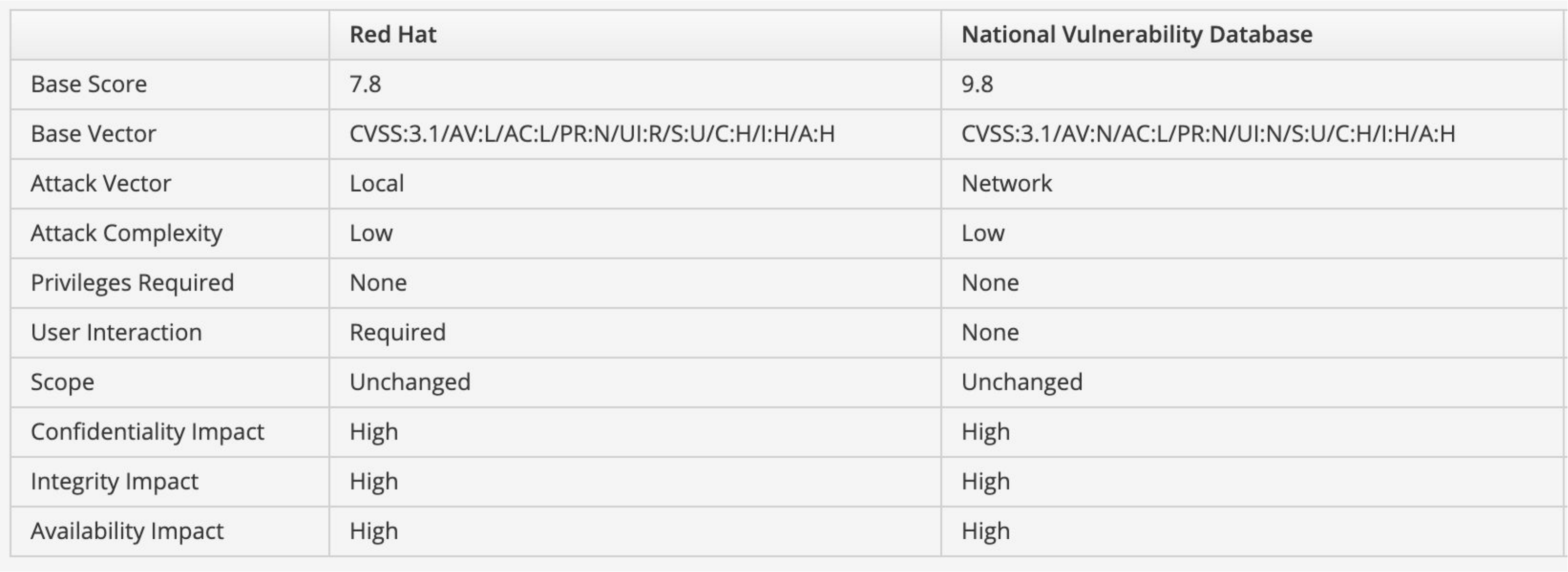
The CVSS Base Score should be supplemented with an analysis of the environment (Environmental Metrics), and with attributes that may change over time (Threat Metrics).

For an organization that employs automated methods to comprehensively utilize the Environmental and Threat metric groups, the resulting CVSS-BTE score can be considered much closer to “Risk”.

Source: FIRST CVSS v4.0 user guide
https://www.first.org/cvss/v4.0/user-guide

CVE-2024-39331 - emacs

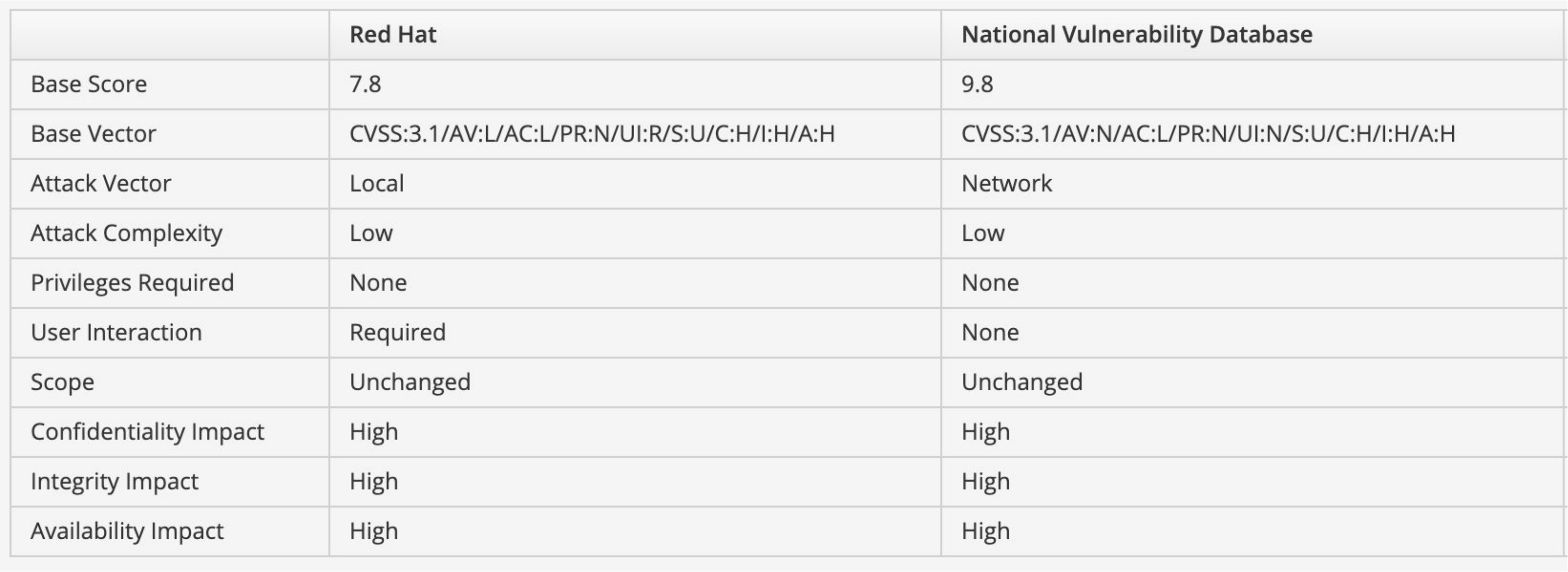
A flaw was found in Emacs. Arbitrary shell commands can be executed without prompting when an Org mode file is opened or when the Org mode is enabled, **when Emacs is used as an email client**, this issue can be triggered when **previewing email attachments**.



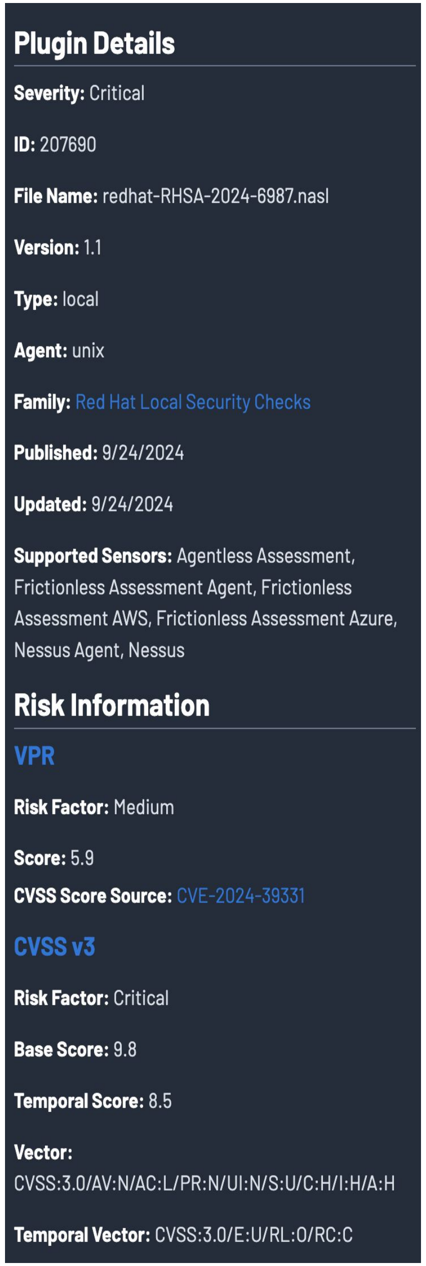
	Red Hat	National Vulnerability Database
Base Score	7.8	9.8
Base Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Attack Vector	Local	Network
Attack Complexity	Low	Low
Privileges Required	None	None
User Interaction	Required	None
Scope	Unchanged	Unchanged
Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High

CVE-2024-39331 - emacs

A flaw was found in Emacs. Arbitrary shell commands can be executed without prompting when an Org mode file is opened or when the Org mode is enabled, **when Emacs is used as an email client**, this issue can be triggered when **previewing email attachments**.



	Red Hat	National Vulnerability Database
Base Score	7.8	9.8
Base Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Attack Vector	Local	Network
Attack Complexity	Low	Low
Privileges Required	None	None
User Interaction	Required	None
Scope	Unchanged	Unchanged
Confidentiality Impact	High	High
Integrity Impact	High	High
Availability Impact	High	High



Plugin Details

Severity: Critical

ID: 207690

File Name: redhat-RHSA-2024-6987.nasl

Version: 1.1

Type: local

Agent: unix

Family: Red Hat Local Security Checks

Published: 9/24/2024

Updated: 9/24/2024

Supported Sensors: Agentless Assessment, Frictionless Assessment Agent, Frictionless Assessment AWS, Frictionless Assessment Azure, Nessus Agent, Nessus

Risk Information

VPR

Risk Factor: Medium

Score: 5.9

CVSS Score Source: CVE-2024-39331

CVSS v3

Risk Factor: Critical

Base Score: 9.8

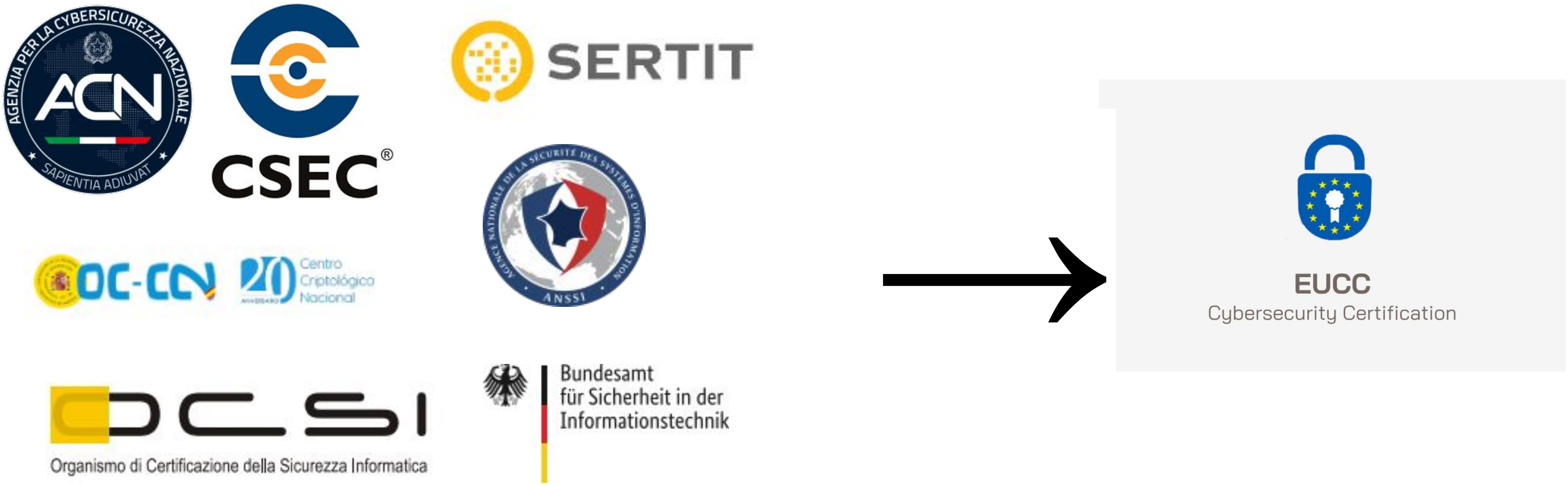
Temporal Score: 8.5

Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

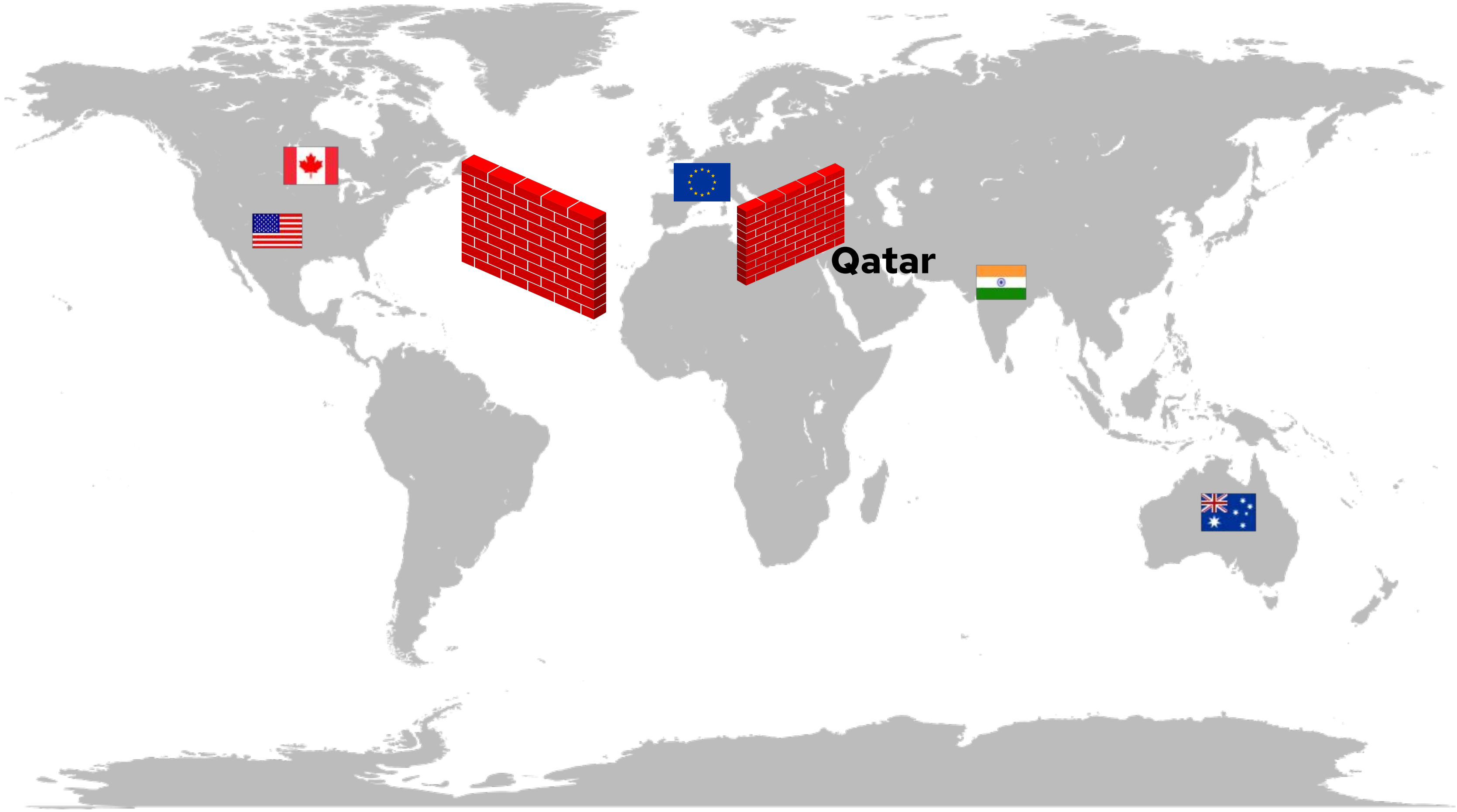
Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

Reciprocity and cooperation

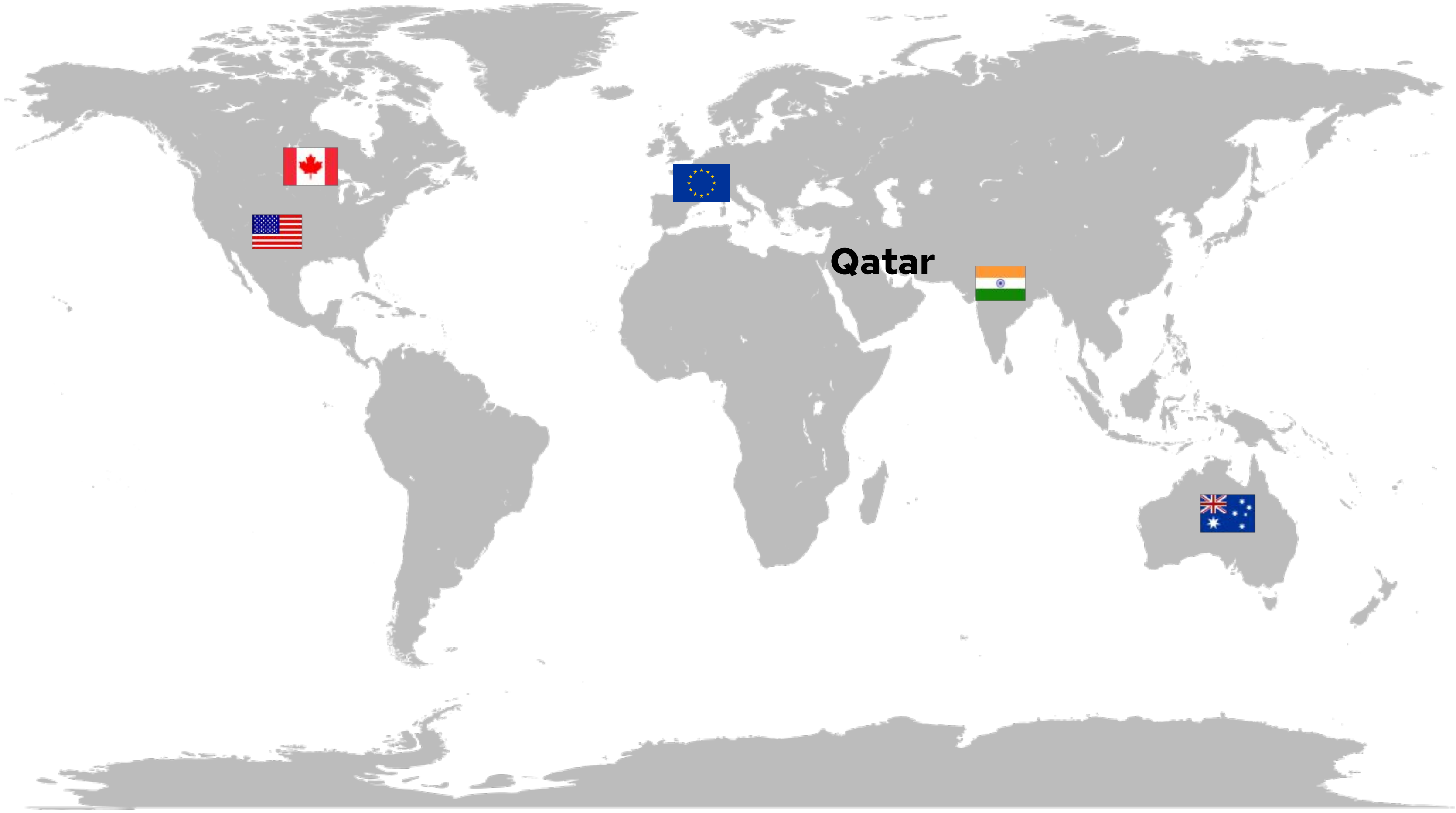
Reciprocity and cooperation


AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT
CSEC®
SERTIT
OC-CCN
20 ANIVERSARIO
Centro Criptológico Nacional
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI
OCSI
Organismo di Certificazione della Sicurezza Informatica
Bundesamt für Sicherheit in der Informationstechnik
EUCC
Cybersecurity Certification

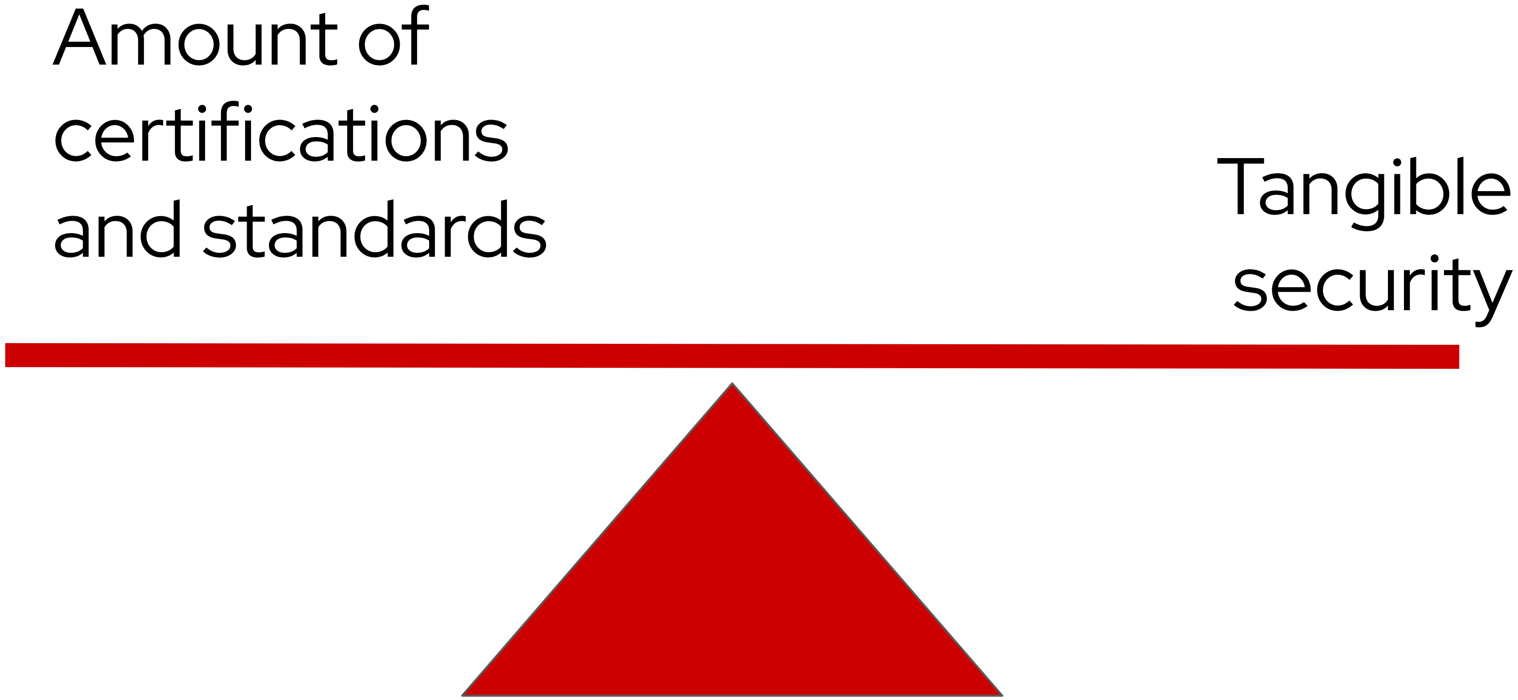
Reciprocity and cooperation



Reciprocity and cooperation



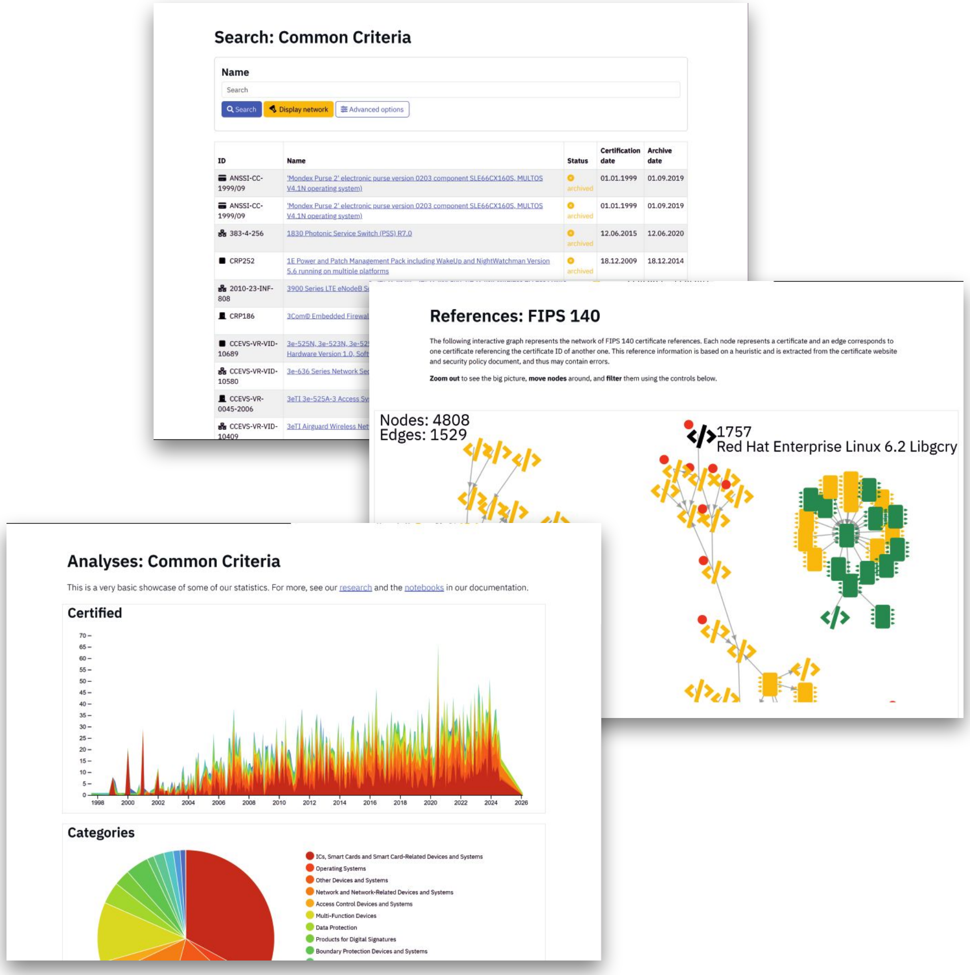
And even more of controversy?



Amount of certifications and standards

Tangible security

Invite: For good evaluation, we need data



Search: Common Criteria

Name

Search

ID	Name	Status	Certification date	Archive date
ANSSI-CC-1999/09	'Mondex Purse 2' electronic purse version 0203 component SLE66CX160S, MULTOS V4.1N operating system)	archived	01.01.1999	01.09.2019
ANSSI-CC-1999/09	'Mondex Purse 2' electronic purse version 0203 component SLE66CX160S, MULTOS V4.1N operating system)	archived	01.01.1999	01.09.2019
383-4-256	1830 Photonic Service Switch (PSS) R7.0	archived	12.06.2015	12.06.2020
CRP252	1E Power and Patch Management Pack including WakeUp and NightWatchman Version 5.6 running on multiple platforms	archived	18.12.2009	18.12.2014
2010-23-INF-808	3900 Series LTE eNodeB S			
CRP186	3Com© Embedded Firewal			
CCEVS-VR-VID-10689	3e-525N, 3e-523N, 3e-52 Hardware Version 1.0, Soft			
CCEVS-VR-VID-10580	3e-636 Series Network Se			
CCEVS-VR-0045-2006	3eTI 3e-525A-3 Access Sy			
CCEVS-VR-VID-10409	3eTI Airguard Wireless Net			

References: FIPS 140

The following interactive graph represents the network of FIPS 140 certificate references. Each node represents a certificate and an edge corresponds to one certificate referencing the certificate ID of another one. This reference information is based on a heuristic and is extracted from the certificate website and security policy document, and thus may contain errors.

Zoom out to see the big picture, **move nodes** around, and **filter** them using the controls below.

Nodes: 4808
Edges: 1529

Analyses: Common Criteria

This is a very basic showcase of some of our statistics. For more, see our research and the notebooks in our documentation.

Certified

Categories

ICs, Smart Cards and Smart Card-Related Devices and Systems
Operating Systems
Other Devices and Systems
Network and Network-Related Devices and Systems
Access Control Devices and Systems
Multi-Function Devices
Data Protection
Products for Digital Signatures
Boundary Protection Devices and Systems

sec-certs

Red Hat booth

Monday–Tuesday, exhibition space

Enhancing Transparency: Insights From the CC Certification Ecosystem

Vashek Matyas, Monday 15:00 (L12b)

MASARYK UNIVERSITY

Red Hat Research

Thank you!