A tale of Two Reports

The Trivial Things We're Told vs. The Vital Things We're Not

Barbhack, Toulon, 08/30/25

Thanks, staff

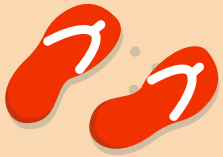
Merci les orgas, merci la régie, merci les bénévoles,
merci la cuisine, merci Toulon, merci les Sponsors...
et merci le public !

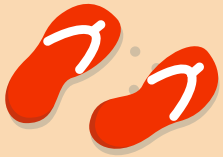
Dark Night Call. Around 3am.
A man is searching for something under the lone street light.
He lost his car keys in the parking lot.

The Street Light Effect

We've got EDR, NDR, MDR, XDR, we have SIEM, SOAR, CASB, SASE ...

We're nearly running out of letters in the alphabet. And still, ***we're looking under the spotlight*** .





Our security posture is a giant, advanced fire alarm system... installed in a swimming pool. It's loud, it's wet, and **yet we completely miss the sharks** .

ISSP / Vuln Mgmt Policy: a "*Severity-based Time To Fix*" became "*CVSS-Score Based Time-to-Fix*"

–Anyone in the room ?

Which one to fix ?

U

CVE-2017-17551

Base Score: 8.8 HIGH
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

K

CVE-2020-15501

Base Score: 6.5 MEDIUM
Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

C

CVE-2017-17692

Base Score: 7.5 HIGH
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

F

CVE-2025-6260

Score: 9.4, CRITICAL
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Which one to fix ?

THERMOSTAT

F

CVE-2025-6260

Score: 9.4, CRITICAL
CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Which one to fix ?

U

CVE-2017-17551

Base Score: 8.8 HIGH
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

VENDING MACHINE

Which one to fix ?

COFFEE !!!

C

CVE-2017-17692

Base Score: 7.5 HIGH
Vector:
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Which one to fix ?

K

CVE-2020-15501

Base Score: 6.5 MEDIUM
Vector:
CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

FRIDGE

Our top talent is now the first line of defense for the snack machine.

Cult of the CVSS Score

It's **easy**, everyone understand the scale.
It's **normalized** , everyone can use the calc.
It's even **automated** / automatable.
Yet, it's **not personalized** .
(still, I do care about the Coffee Machine)

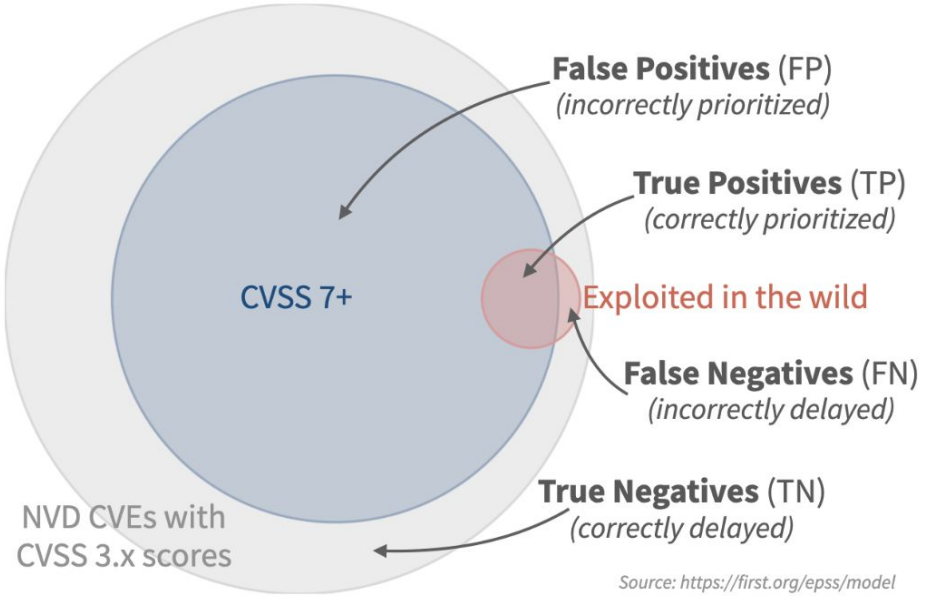
Better things to do:

- ***Move*** the Coffee Machine out of the network
- Do ***risk tagging*** to minimize absolute scores
- ***Use*** contextualized score, like **EPSS**, which tries to integrate the ***exploitability***

Performance: Remediating CVSS 7 and above

Looking at the performance of CVSS scores produced October 1st, 2023, comparing against the observed exploitation activity recorded from Oct 1st to Oct 30th, 2023. CVSS threshold is (arbitrarily) set at 7.

Our Decision…	Exploitation Activity… Observed	Not Observed
Remediate (CVSS 7+)	3,166 (2.3%) *True Positives (TP)*	76,858 (55.1%) *False Positives (FP)*
Delay (< CVSS 7)	686 (0.5%) *False Negatives (FN)*	58,763 (42.1%) *True Negatives (TN)*



src: https://www.first.org/epss/

Why lose time while our data are encrypted ?

Apologies ?

Do you ever go to the car mechanic telling them you've got to change the connecting rod ?

Don't waste time with precision when no precision is required.

"Et sérieusement les gens, parlez français. Merci."

Tolérance, Inclusivité, Nationalisme, Ouverture, *anyone* ?

For us, it's like mail

Spam

Obvious noise you don't like

"Meet the Anonymous
in your region"

Phishing

Obvious attacks you discard

"You have again winned $15M through the national lottery this Thursday [1]"

[1] (draws are on Mon., Wed. and Sat.)

Mailing lists and notifications

Good mail, good information. Most of them I don't want anymore, though.

Our SOCs have become professional unsubscribers for security newsletters nobody wants


The noise to bring them all, and in the
chaos, bind them

Missed Notifs

Target, 2013

Consequences : 200 HERE ARE CREDIT CARD INFO FOR 70m CUSTOMERS

Vector : Fazio Mechanical Services, a third-party HVAC vendor

Missed Notification : FireEye detected the initial breach and the movement of the attackers within the network, flagged it as suspicious and issued alerts. The security team either dismissed them as false positives.

Rouen, 2019

Consequences : 404 HOSPITAL NOT RESPONDING

Vector : Phishing

Missed Notification : Virus Alert, single computer. It can be a ransomware since it's on a single computer. Then: "*Living off your land*", they used internal tools, *then* they ransom'd

Colonial Pipeline, 2021

Consequences : 204 NO MORE FUEL

Vector : Account Takeover

Missed Notification : Probably an impossible traveler notification which was not deemed as important. A non-blocking alert, coupled to a lack of MFA.

Silent Ghosts

NSA, 2016

Consequences : 200 HERE ARE YOUR DATA

Vector : An employee using a NSA USB Key to... exfiltrate NSA data.

Missed : NSA was poorly looking at what actual employees did (3yrs after Snowden)

SolarWinds, 2019

Consequences : 500 CI/CD NOT AVAIL

Vector : *Living of your Land*

Missed : Third-Party Vendor Management, customers of SolarWinds were very confident in SolarWindws (reminder: *CircleCI, Dec., 2023*)

Kiabi, 2024

Consequences : 100M€

Vector : I'm a accountant, I make accounting

Missed : Who controls the controllers ?

But the scariest part is what's NOT in your inbox. The noise is bad. It burns us out. But it's not the biggest danger. The biggest danger... is the silence.

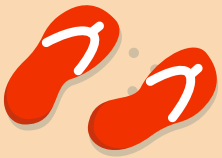
"I wasn't sure if this is indeed a security risk": Data-driven Understanding of Security Issue Reporting in GitHub Repositories of Open Source npm Packages

Rajdeep Ghosh, Shiladitya De, Mainack Mondal

June 2025

10,907,467

PR analyzed in Open Source Projects



Some stats

0.13%

TAG::Security

aka Developer declares they fixed a security issue

14.8%

are missing TAG::Security

A grand total of 1,617,738 security-related issues

1/113

ratio of CVE'd vulns

aka Security Issues that will never get a CVE

Silly Bounties

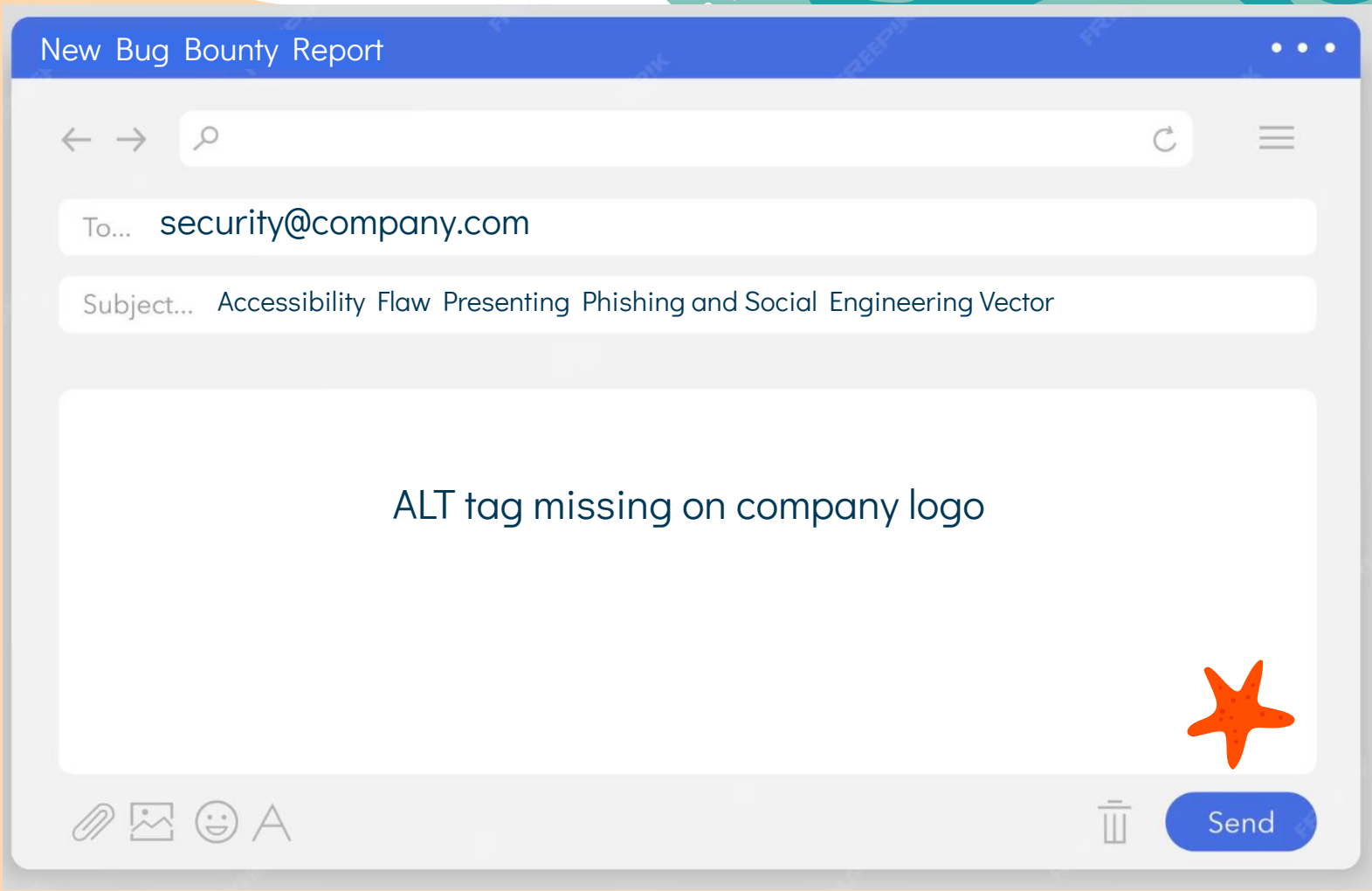
New Bug Bounty Report

To... security@company.com

Subject... Unencrypted Traffic Vector Puts User Data at Risk of Man-in-the-Middle Attacks

Lack of HSTS headers

Send


New Bug Bounty Report
To... security@company.com
Subject... Accessibility Flaw Presenting Phishing and Social Engineering Vector
ALT tag missing on company logo
Send

New Bug Bounty Report

To... security@company.com

Subject... Sensitive Directory Traversal and Information Disclosure via Misconfigured File on Webserver

robots.txt

Send

New Bug Bounty Report

To... security@company.com

Subject... Critical Information Disclosure via Unrestricted File Access

S3 Bucket open to public, it contains our marketing PDFs and user profile pictures.

Send

New Bug Bounty Report

To... security@company.com

Subject... Sensitive API Key Exposure Leading to Potential Data Leak

Your Google Maps API Key has leaked

Send

New Bug Bounty Report

To... security@company.com

Subject... Unauthorized Account Provisioning Due to Unverified Email Registration

I can create an account with a non-existing email

Send

New Bug Bounty Report

To... security@company.com

Subject... Source Code Information Leakage Threat

"Comments in HTML Code"

Send


Swim well. Don't drown. Have fun.
Hack the planet ♡

Thanks!

Do you have any questions?

Seb, aka **Koreth**
Informaticien dans ton cinéma

@linkedin.com/reboot
@Barbhack: Spot the Kilt Guy