THE CASE FOR A BUG BOUNTY PROGRAM OF LAST RESORT

REVISITING THE ECONOMIC VALIDATION FOR BUG BOUNTY PROGRAMS

Chair of Entrepreneurial Risks D-MTEC, ETH Zurich

Stefan Frei, Oliver Rochford

https://techzoom.net/bug-bounty-reloaded

Abstract

This paper makes the case for a centralized Bug Bounty Program of Last Resort.

A larger number of vendors either lack the maturity, funding or incentive to invest more in secure software development, meaning that a) we do not really know the true number of vulnerabilities out there - resulting in a shadow population of vulnerabilities b) large parts of our digital economy and infrastructure are at risk from this shadow population of vulnerabilities c) the digital transformation is jumping without a parachute, with few universal mechanisms in place to ensure minimum standards and safe innovation.

Minimal software quality standards are far and few between and have also been notoriously difficult to enforce and quantify. Bug bounties have instead proven themselves an additional effective mechanism to improve vulnerability discovery, while also reducing the availability of zero-day vulnerabilities and exploits to malicious cyber actors. But they are not trivial to operate and have not yet been adopted widely or consistently. Startup vendors and open-source projects especially are challenged to fund and manage such programs, yet their technologies underpin the digital transformation.

A **bug bounty program** rewards researcher reporting vulnerabilities to the vendor of the affected software in the form of financial compensation

Our analysis proposes and validates a model for a broader scope bug bounty program (Bug Bounty of Last Resort) by assessing and comparing the cost of having a massive vulnerability purchase program following a coordinated disclosure process - and comparing this cost to cybercrime losses.

Key Findings

Financing a bug bounty program of last resort that offers competitive and lucrative compensation for vulnerability discovery and innovative defensive tools is affordable. The benefits outweigh the costs, especially when calculated as a percentage of GDP (EU, US) compared to the cost of cyber security and damages resulting from cybercrime

- A **shadow population of zero-day vulnerabilities** exists due to a lack of consistent investment in vulnerability discovery.

- Costs for vulnerability exposure have been fully externalized to end users, **who are unable to quantify or manage the risk** from the shadow population of vulnerabilities.

- Bug Bounty Programs have been adopted successfully to improve vulnerability discovery by select vendors - but have not been adopted industry-wide **due to lack of incentives, regulatory guidance, or affordability**.

    - Less than 50 vendors account for more than 50% of annually disclosed vulnerabilities
    - Many software suppliers who would benefit most, **critical open-source projects and smaller vendors**, cannot fund them.

- Our proposal, an industry-wide **Bug Bounty Program of Last Resort (BBPLR)** expanding coverage to all critical technologies and vendors will reduce the risk posed by shadow vulnerabilities and reduce the pool of vulnerabilities available for cyber criminals to exploit.

- Economically, a BBPLR is easily affordable while measurably improving the rate of vulnerability discovery to ultimately reduce the shadow vulnerability population and systemic risk.

- The cost of **1,732 Billion to purchase 81% of all medium to critical severity vulnerabilities in 2020** for 50k/150k, and 250k USD would be **much less than 0.1% of the GDP of the OECD, the EU, or the US**.

- Purchasing vulnerabilities at scale **makes economic sense if it reduces the overall losses to cybercrime by at least 0.5%** (zero-point-five percent per USD 1,000 billion)

Table of Contents

1. There is no such thing as secure software

Vulnerability disclosures have exceeded escape velocity.
Vulnerabilities in software, usually defined as a weakness or flaw in an application or IT infrastructure that a malicious user can abuse to compromise a system, are a key component of most data breaches. Yet historically users and implementers, not vendors, have been responsible and liable for mitigating the risk from vulnerabilities.

The volume and velocity of new vulnerability disclosures that organizations must address have been inexorably increasing for more than two decades. Information security management frameworks and regulations do commonly include requirements to manage vulnerabilities, and organizations have invested more and more into cyber hygiene. But the sheer amount and diversity of software used by a typical enterprise means that we are chasing a moving target. Operationalizing vulnerability management has become a scalability and prioritization challenge. More importantly, it is predicated on vulnerabilities being disclosed and known, which requires active discovery and research.

An estimated **18,000 vulnerabilities affecting 2,900 vendors** were published in 2020. The top 10 vendors typically account for 35% and the top 50 vendors for 57% of all published vulnerabilities.

Only a few vendors account for most of the volume as shown in Table 1 and Figure 1 below. Typically, the top 10 vendors account for 35% and the top 50 vendors for 57% of all published vulnerabilities per year.[1]

ALL VENDORS		TOP-N VENDORS					
VOLUME		SCOPE	VOLUME		SHARE	GROWTH	
2010	2020	Vendors	2010	2020	in 2020	10 yrs	**p.a.**
4'639	18'335	**Top-10**	1'903	6'418	**35%**	x 3.37	**x 1.13**
		Top-50	2'587	10'441	**57%**	x 4.04	**x 1.15**
		Top-100	2'877	11'840	**65%**	x 4.12	**x 1.15**
		Top-500	3'816	14'864	**81%**	x 3.9	**x 1.15**

Table 1 - Year-over-year growth of vulnerability disclosures of 13% - 15% in the past decade for all groups of vendors (top-10 to top-500). In 2020 the top 10 (of 2,900) vendors accounted for 35% of all vulnerabilities published. Source NVD [1]

Overall, the volume of new vulnerabilities has consistently grown by double digit percentages year on year. While some vulnerabilities arise out of bad development practices and may be eliminated by applying best practices such as secure Software Development Lifecycle (SDLC) management, others are a result of software complexity. There is also a misalignment in economic incentives for software suppliers to invest in security, also contributing to the continuous flood of new vulnerabilities.

[1] The term vendor is used to refer to the producer of software, regardless of whether that software is sold commercially

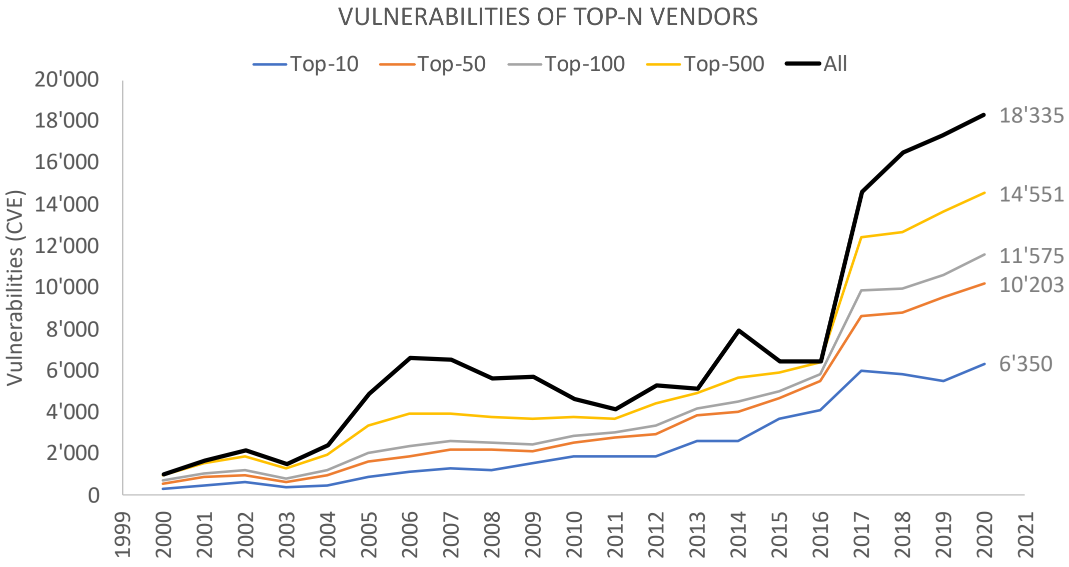


Figure 1 - Number of vulnerabilities (CVE entries) disclosed per year for the top 10 to top 500, and all vendors. In 2017, the number of entries jumped significantly. Much of this 2017 expansion is due to the increased capability of the program that manages the CVE process feeding the National Vulnerability Database (NVD). [2]

With few incentives to invest in secure software design, and even fewer penalties or liability costs [3] for releasing insecure software, it has become common to prioritize commercial agility rather than security. The risk has thus been fully externalized.

VULNERABILITY

A weakness of software, hardware or online service that can be exploited. A vulnerability itself does no harm, but if exploited it typically results in unwanted consequences.

Without product liability for software, the cost of mitigating vulnerabilities is externalized as risk and cost to end users and businesses. Security updates must be viewed as product recalls for defective software at the user's expense, something that is unacceptable in other industries like automotive or aviation. At the same time, abuse of known (and yet-unknown) vulnerabilities in software by cyber criminals and nation state actors has risen, with the global cost of cybercrime in the order of billions of USD per year [4].

One thing to note is the unequal investment and focus spent on vulnerability discovery and mitigation across the industry. A vendor that invests more in vulnerability discovery and disclosure can appear to have more vulnerabilities than a vendor that does not.

1.1. Current and emerging approaches to handling & reducing vulnerabilities

Building security into the Software Development Lifecycle (SDLC) is still the most effective method of minimizing vulnerabilities in software code. Building a mature and effective secure SDLC requires investment of time, resources and relies on a high level of expertise. Emerging and open-source vendors especially are challenged to develop, operate, and finance effective code level security programs. And even a mature SDLC program will miss some flaws due to code complexity and commercial pressures.

Fashionable business philosophies, for example the focus on time to market, and “move fast and break things”, also prioritize speed and agility over secure code development.

To compensate, the cybersecurity industry has developed additional methods of information sharing, self-policing and investment in handling vulnerability discoveries. Two of the more successful and prevalent approaches include **Coordinated Vulnerability Disclosure** [5] and **Bug Bounty Programs**.

COORDINATED DISCLOSURE

Ethical researchers discovering a vulnerability coordinate the disclosure with vendors to allow a fix to be developed and released.

1.2. Coordinated disclosure

In Coordinated Disclosure, also known as Responsible Disclosure, ethical researchers discovering a vulnerability coordinate the disclosures with vendors. This ensures that a security update is available in parallel to disclosure. If a vendor does not cooperate within a reasonable timeline, the vulnerability is usually still published (**Full Disclosure**) so that those affected by it can at least assess the associated risks and deploy mitigating controls. Typically, the vendor credits the researcher for finding and reporting the vulnerability.

Pro’s	Con’s
• Vendor has time to develop a patch • Public and peer recognition for the researcher • Vendors benefit from 3rd party expertise and effort • Standards: vulnerability disclosure ISO 29147 and vulnerability handling processes ISO 30111	• Ad-hoc and unstructured • Relies on the altruism of finder • No financial incentive for ethical behavior • Risk of legal threats against finder [6]

A considerable percentage, if not the majority, of disclosed vulnerabilities are discovered by unpaid volunteers, including independent researchers, vendors, and end users. The cyber security community has a long tradition of intelligence sharing, with incentives such as peer group recognition. In addition, industry and community full disclosure is also a response to an overwhelming real-world problem that no individual company or organization can solve alone.

Coordinated Disclosure also requires the willing participation of vendors, which can vary. To highlight an example, in 2015, 94% of the Forbes Global 2000 had no formalized way for security researchers to report a security issue [7]. Even when such a policy exists, Ethical Hackers have reported that they are sometimes reluctant to submit vulnerabilities due to threatening legal language [8]. While some companies actively discourage and disincentivize any disclosure of a vulnerability in their service or product through the threat of legal measures, others may

FULL DISCLOSURE

Publication of full details of a vulnerability with or without coordinating with the affected vendor.

encourage submissions but disincentivize these through onerous legal restrictions such as a lack of discovery credit, non-disclosure agreements or broken processes.

Participation can also be encouraged, for example through a well-publicized and supported coordinated disclosure program. But, to incentivize broader participation in coordinated disclosure, mature vendors have started initiating Bug Bounty Programs.

In 2015, **94% of the Forbes Global 2000 had no formalized way** for security researchers to report a security issue

1.3. Bug bounty programs

A bug bounty program offers researchers recognition and compensation for reporting vulnerabilities to the vendor of the affected software (either directly or through a broker). Bug bounties have become increasingly popular in recent years, even the US Department of Defense relies on bug bounties to secure their infrastructure [9]. To cite a high-profile example, in the Hack the Air Force bug bounty program, it took less than a minute for the first valid vulnerability to be reported [10].

Pro’s	Con’s
• Vendors have time to develop a patch • Public recognition of finder • Stimulate research into software security • Attracts diverse hackers - diversity of crowd means diversity of skills and expertise • Incentivizes ethical behavior, internalizes cost of vulnerabilities • Can be more effective in finding some types of vulnerabilities than internal research **[11] [12]**	• The system can be, and is gamed: • Rogue developers write vulnerabilities to later report them for profit • Automated discovery of low hanging fruit • High overheads to manage submissions • Are vulnerabilities in software depletable (spares or dense)? • More complex and sophisticated vulnerabilities are neglected

Bug Bounty Programs have traditionally been reactive and focused solely on compensating for software vulnerabilities. Recent research [13] has shown that compensating researchers for innovative defensive tools such as automating vulnerability discovery, or exploit mitigation techniques, is more proactive and yields greater return of investment.

EXPLOIT

An exploit is a piece of software, a set of data, or sequence of commands that takes advantage of a vulnerability in order to cause unintended or unanticipated behavior to occur in software or hardware.

2. Limitations of and gaps in current approaches

Economic incentives can play a key role in vulnerability disclosure, regardless of what type of vulnerability disclosure process is ultimately pursued [13].

2.1. Inconsistent coverage due to viability and affordability

Due to the voluntary aspect of Coordinated Disclosure and Bug Bounty programs, coverage is inconsistent. The security-haves for example, Google, Microsoft, or Apple, have mature and well-funded Bug Bounty Programs. On the other end of the spectrum, we have the security-have-not's, for example emerging vendors and open-source projects who lack the resources to fund and manage Bug Bounty programs (recent examples demonstrating how important this last aspect, are in the Appendix under Software Supply Chain).

REWARDING VULNERABILITY DISCOVERY & VULNERABILITY DEFENSE TOOLS

When we refer to Bug Bounty Programs in this paper, we implicitly include compensating researchers for vulnerabilities and for defense tools and methods.

Affordability is a major factor. The cost of a bug bounty program represents only a small percentage of a larger vendors' revenue (see Table 5) while software suppliers with lower or no revenue (open-source) cannot afford such initiatives.

A further inhibitor is that some vendors may also pursue a “Security through Obscurity” strategy or wish to obfuscate security issues for competitive reasons. While the latter is understandable, it comes at the cost of end user, economic and societal security.

This results in only partial coverage of software in private and enterprise use. This discrepancy does not just apply to being able to manage and fund such programs, but also being able to respond to the disclosed vulnerabilities and having the resources to develop a patch or fix.

2.2. Competition by the grey market in zero-days and vulnerabilities

Most data breaches that a typical enterprise experiences may not involve zero-day vulnerabilities, even if their usage has risen in the past year [14]. But attacks that do leverage zero-days are typically targeted against sensitive and hardened targets, such as critical infrastructure and national security.

ZERO-DAY

A vulnerability that has not been publicly disclosed. In some definitions a vulnerability for which no patch or fix has been publicly released.

Zero-days are known only to a handful of operators, have not been publicly disclosed and subsequently have no mitigations available. Due to their effectiveness in attacking even hardened targets, a shadow market has developed for their trade offering prices more than USD 1 Million for select zero-day exploits targeting prevalent software.

The greatest challenge that bug bounty programs face is the competition with the criminal and unregulated markets in zero-days and vulnerabilities.

While the number of actors in the criminal market for zero-days has shrunk considerably due to the impact of professionalized exploit brokerages, there is still a small but profitable segment catering to the cybercrime-as-a-service supply chain. The criminal market has become focused on special purpose vulnerabilities rather than headline grabbing zero-days unable to compete for prime exploits against the better funded brokers.

The prices for exploits in the unregulated, extralegal market (usually associated with nation state actors) have exploded over recent years, with some exploits nominally fetching millions of dollars, for example for mobile communications [15]. As these vulnerabilities are of interest to nation state actors for national security purposes, they tend to focus on critical technologies, and worst of all from a defender's point of view, disappear from public knowledge until accidentally disclosed or used in an attack [16]. Another aspect to consider is that any advantage gained through non-disclosure of zero-days is also an illusion. Almost every nation state actor is a glass cannon in cyber war. You can successfully attack, but not defend. And while you know which exploits you possess; information asymmetry means you do not know if others exist and who possesses them.

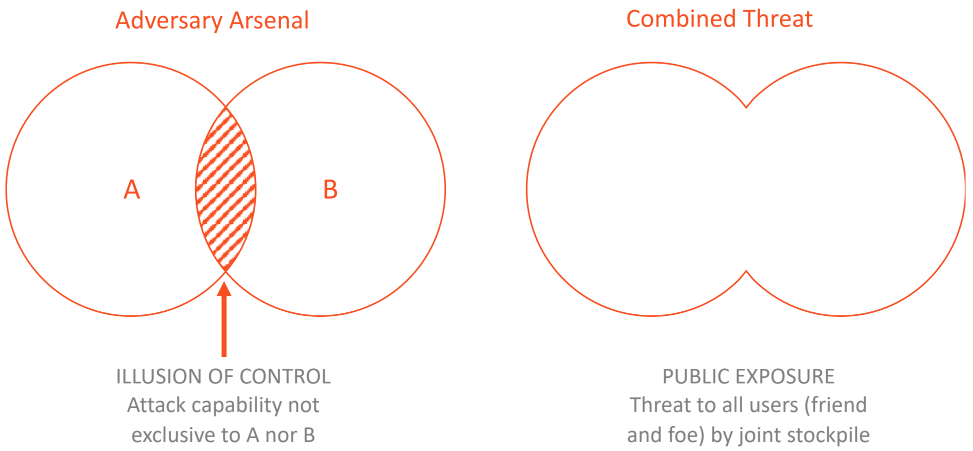


Figure 2 - Adversaries A and B stockpile zero-day vulnerabilities, but their knowledge is not exclusive. A single adversary can never be sure if they exclusively own a vulnerability or exploit. While being kept secret, software vendors cannot patch the vulnerability and the exposure increases for all society (including the stockpiling actors). We are exposed to all possible stockpiled exploit arsenals.

Due to the large sums involved, these vulnerabilities represent the greatest challenge to solve with bug bounties, and also create a paradox: it impacts our allies and adversaries both equally.

3. Bug Bounty Program of Last Resort

This paper makes the case for a centralized bug bounty program of last resort. By centralized we mean that it is operated by a central authority, for example government or industry-wide association, and collectively rather than on a per-vendor basis. By last resort we mean that relevant and critical software and technology is included, to extend coverage to start-ups, open-source, and vendors with less mature security programs.

In our model, the Bug Bounty program of last resort will buy all published vulnerabilities of critical, high, and medium severity. The purchase price increases with the severity of the vulnerability.

Bug bounties have proven themselves an effective mechanism to reduce the availability of zero-day vulnerabilities and exploits [17], but are costly to implement and have not been adopted consistently. Startup vendors, smaller vendors and open-source projects especially are challenged to fund and manage such programs, yet their technologies are used widely and underpin the digital transformation.

To effectively address the larger problem of discovering vulnerabilities, will require several reinforcing and interacting bottom-up and top-down mechanisms:

- If vendors are given misaligned incentives, society will have to carry the cost and risk of high and growing volumes of vulnerabilities
- Responsibility, Liability and Incentives must be shared between users, vendors and government. This is not only a question of fairness, it's a matter of effectiveness.
- Attribution and internalizing of vulnerability cost are a key lever to change
- Absence of evidence is not evidence of absence and we cannot manage what we cannot measure [18]

3.1. Economics of bug bounty cost

To validate the limits and economic feasibility of a bug bounty program of last resort we model the cost of purchasing vulnerabilities at large scale and at competitive prices. We model two scenarios with vulnerability and economic data covering the past 10 years. Our analysis proposes and validates a model for the affordability of broader scope bug bounty programs by assessing and comparing the cost to:

- the GDP of major economic regions such as OECD, EU, US, and Asia
- the estimated yearly losses to cyber crime
- the typical security expenditures in other industries
- the revenue to the software vendor in the same year

We assume global cybercrime losses of USD 1,000 billion per year (estimates of the global cost of cybercrime are always a matter of debate and range from USD 100 to 6,000 billion) [4] [18].The cost of the NotPetya malware that spread from an Ukrainian firm to the largest business worldwide in 2017 alone is estimated to be 10 Billion USD [19].

VULNERABILITY PRICE BY SEVERITY

	MEDIUM	HIGH	CRITICAL
Price per vulnerability USD	50'000	150'000	250'000
CVSS score	4-4.9	7-8.9	9-10

Table 2 - Purchase price based on the severity of the vulnerability derived from the common vulnerability scoring system (CVSS) published in the NVD [20]

This pricing structure aims at systematically capturing most critical vulnerabilities covering all technologies across vendors.

Bug bounty programs actively enable **information sharing**, **capacity building**, **training**, and **providing transparency** for all stakeholders - industry, society, and national securitv.

Typical industry bug bounty prices are much lower than the prices of our model. Only exceptional and rare vulnerabilities are rewarded with more than 250k for coordinated disclosure or more than 1 Million for government use. We assume that our model prices would attract a large proportion of capable security researchers and lead to increased security research and tool creation. It would also drive the cost of zero-days up - raising the ceiling of entry for cyber criminals and **nation state actors**.

We believe that vulnerabilities are sparse enough for a bug bounty of last resort to be effective. Every vulnerability either meaningfully lowers the number of vulnerabilities that are extant or rises the effort and complexity to find further vulnerabilities. The growth of bug bounty programs witnessed over the past 10 years demonstrates the effectiveness of bug bounties to increase security and identify vulnerabilities proactively [21].

3.2. Model A - Purchasing all vulnerabilities

In Figure 3 we model the yearly cost to purchase all medium to critical security vulnerabilities of the top-10 to top-500 vendors since 2000. This model covers between 35% (top-10) to 81% (top-500) of the vulnerabilities disclosed per year. In Table 3 we compare the purchase cost of 2020 to the most recently reported GDP of major economic regions and the estimated yearly cost of cybercrime. In Table 4 we compare the cost to global spend in IT.

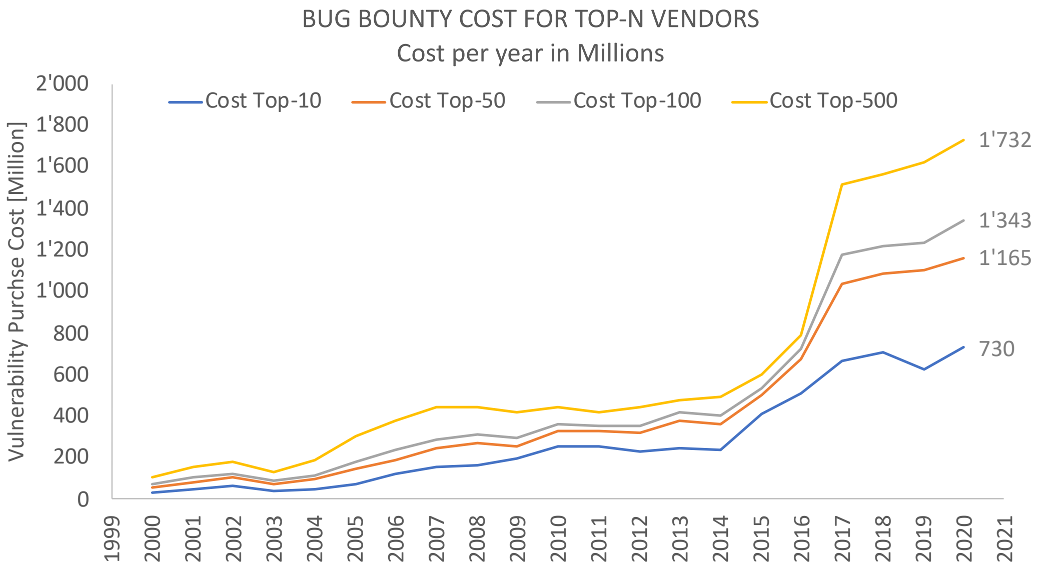


Figure 3 - Shows the price to purchase all vulnerabilities of the top 10, top 50, top 100 and top 500 vendors which account for 35%, 57%, 65% and 81% of all medium to critical severity vulnerabilities published in 2020. The purchase price is modeled as USD 250k for critical, 150k for high, and 50k for medium severity vulnerability. Data source and severity rating from NVD.

BUG BOUNTY COST COMPARISON									
VULNERABILITIES				PURCHASE	PERCENT OF GDP OR LOSSES TO CYBER CRIME				
Vendors	CVE Top-N	CVE All	Share	Cost Mio	OECD	EU	US	EAS	Cyber Crime
Top-10	**6'418**	18'335	35%	**730**	0.0014%	0.0047%	0.0034%	0.0027%	0.0730%
Top-50	**10'441**	18'335	57%	**1'165**	0.0022%	0.0075%	0.0055%	0.0043%	0.1165%
Top-100	**11'840**	18'335	65%	**1'343**	0.0025%	0.0086%	0.0063%	0.0050%	0.1343%
Top-500	**14'864**	18'335	81%	**1'732**	0.0032%	0.0111%	0.0081%	0.0064%	0.1732%

Table 3 - Yearly cost in Million of buying the top N vendors vulnerabilities compared to the 2019 GDP of OECD, EU, US, and East Asia & Pacific regions and losses to cyber crime

The cost of 1,732 Billion to purchase 81% of all medium to critical severity vulnerabilities in 2020 would be

- **much less than 0.1% of the GDP of major economic regions**
  less than 0.005% of the cumulated GDP of OECD members, or 0.02% of the cumulated GDP of EU members, or 0.01% the US GDP, or 0.01% of the East Asian & Pacific states.
- **much less than 0.5% of global cybercrime losses**
  assuming the total losses amount to USD 1,000 billion
- **much less than 0.1% of global spend on IT**

Purchasing these vulnerabilities makes economic sense if the indirect losses of cybercrime are thereby reduced by at least 0.5% (zero-point-five percent).

WORLDWIDE IT SPENDING			
SECTOR	SPENDING [Mio]	BOUNTY [Mio]	SHARE %
Data Center Systems	214'911	1'732	0.81%
Enterprise Software	476'686	1'732	0.36%
Devices	711'525	1'732	0.24%
IT Services	1'040'263	1'732	0.17%
Communicatins Services	1'372'938	1'732	0.13%
Overall IT	**3'816'323**	**1'732**	**0.05%**

Table 4 – Worldwide spend on IT in 2019 compared to cost of buying the top-500 vendors vulnerabilities (81% of all vulnerabilities) per year. Source [24]

Buying all vulnerabilities is not feasible (and not necessary) to extend the benefits of crowdsourcing to the entire digital supply chain, improve vulnerability disclosure effectiveness, and reduce the pool of available zero-days in nation state arsenals.

3.3. Model B - Vendor purchases its vulnerabilities

In this scenario we compare the cost to a specific software vendor to purchase all the vulnerabilities discovered in his products per year. Software vendors may not be incentivized to engage in Coordinated Disclosure or bug bounty programs in the absence of liability for vulnerabilities found in their products or services, or because they are not profit oriented open-source projects.

Comparing the cost of a bug bounty program to the vendor's revenue gives insights into the affordability of any initiative aiming to inter [24]nalize the software vulnerability costs.

Table 5 below compares the cost of purchasing the vulnerabilities of the top-20 vendors in 2020 to their most recently reported yearly revenue or financial results of the trailing twelve months (TTM).

BUG BOUNTY COST COMPARISON - TOP-20 IN 2020

Rank	Vendor	Traded	Com	Open	Bug	Max	CVEs	Cost	Revenue	Share
			mercial	Source	Bounty	Bounty		[Mio]	[Mio]	%
1	Microsoft	MSFT	Yes		Yes	250k	1'272	159	147'114	0.11%
2	Google	GOOG	Yes		Yes	133k	1'215	143	166'030	0.09%
3	Oracle	ORCL	Yes				819	71	39'403	0.18%
4	Netgear	NTGR	Yes		Yes	15k	606	61	1'141	5.35%
5	Cisco	CSCO	Yes		(Yes)	10k	568	63	48'071	0.13%
6	IBM	IBM	Yes				565	50	75'030	0.07%
7	Apple	AAPL	Yes		Yes	1,000k	468	55	273'857	0.02%
8	Adobe	ADBE	Yes				313	43	12'868	0.33%
9	Qualcomm	QCOM	Yes		(Yes)	15k	307	53	19'999	0.27%
10	RedHat		Yes	Yes			306	30	3'362	0.89%
11	Debian			Yes			271	28		
12	OpenSUSE			Yes			249	27		
13	Intel	INTC	Yes		Yes	100k	240	24	78'098	0.03%
14	GitLab		Yes	Yes	Yes	20k	240	21	120	17.50%
15	Jenkins			Yes			230	17		
16	SAP	SAP	Yes				222	20	27'839	0.07%
17	Fedora			Yes			219	22		
18	Huawei		Yes				190	16	132'634	0.01%
19	Mozilla			Yes	Yes	10k	179	19	828	2.29%
20	Canconical		Yes	Yes			162	13	119	10.92%

Table 5 - Top 20 vendors with vulnerability purchase cost and yearly revenue (in Million USD). The list also indicates vendors with a and bug bounty program and the max payout if available. Source: see Appendix.

Market Structure

These top 20 vendors account for the majority of software in private and commercial use, covering all market dominating browsers, operating systems, databases, business process applications, networking hard- and software, mobile devices, and much more. The security of the digital society depends critically on the security efficacy and investments of these vendors.

- Eleven of the top 20 vendors are publicly traded companies, with ten vendors reporting revenues in **excess of USD 10 Billion per year**.
- Five of the top 20 vendors pursue **no commercial interests and have therefore no revenue** - they exclusively depend on sponsoring or the community
- Eight of the top 20 vendors main product is **open-sourced or based on open-source software**
- Nine of the top 20 vendors **have a bug bounty program** of some sort with maximum payouts ranging between USD 15k to 1,000k.
- Seven of the eleven traded vendors have **a bug bounty program**. Qualcoms bug bounty is by invitation only, Cisco's is limited to the Meraki product line.

Financial Impact

Financial impact of a bug bounty program purchasing all of the vendors vulnerabilities compared to the yearly revenue of the vendor

- The cost for the eleven publicly listed vendors to buy their own vulnerabilities is **less than 0.5% of their yearly revenue**[2] (excluding the outlier Netgear[3])
- Three of the four vendors with a cost/revenue share larger than 1% are **based on open-source software** (GitLab, Mozilla, Canonical)
- Four of the top-20 **vendors report no revenues / are not commercial** (Debian, OpenSUSE9, Jenkins, Fedora)

For the year 2016 US-based OEMs and suppliers in the **automotive industry** reported paying approximately **$22 billion of warranty and recall accruals**. Best-in-class supplier companies target approximately **1% for annual recall and warranty costs** combined [23]. GM revenue 2020 (tracking twelve-month TTM): 115.793 Million.

In the United States' retail sector, the accepted rate of "pilferage" or "inventory shrinkage" (considered a cost of doing business) is between 1.5% and 2.0% of annual sales - and much higher than the relative costs for a BB program of last resort [22].

There is considerable room for profitable vendors to accept the responsibility and invest into the security of their products without a risk to their business.

On the other hand, and importantly, non-commercial software vendors cannot afford a bug bounty program on their own, while many commercial products or cloud offerings critically depend on such open-source.

The Internet Bug Bounty addresses this challenge, and our data shows that the industry could easily afford to scale and support this model [23].

The analysis of model A and B demonstrates that a bug bounty program of last resort with offering competitive prices is easily affordable. Even doubling the prices or volume of vulnerabilities purchased would not exceed financial ability of most vendors or economic regions.

Such a bug bounty program shall not be confined to purchase vulnerabilities only. Lucrative rewards for effective and innovative tooling for defense or identification of vulnerabilities shall be included and can be easily afforded.

[2] Cost/revenue share of the 11 publicly traded organizations: average 0.60%, median 0.11% (including Netgear)

[3] Netgear had 1,893 vulnerabilities in 2020 and less than 50 vulnerabilities per year in all the previous years. The reason for the rise in 2020 was not investigated.

3.4. Aspired benefits of a Bug Bounty Program of Last Resort

Cyber attackers have become accomplished in finding the weakest link in an enterprise's security, even if that means focusing on the supply chain, as for example in the recent Solarwinds Breach [24]. Regardless of how much a single vendor invests, or how secure their software is, if there are other vulnerable components available to an attacker, they will gain entry. Even if future regulation may stipulate minimal standards, these will not eliminate all vulnerabilities. Major vendors such as Google, that have very mature security programs, run BB programs - a tacit acknowledgement that despite best intentions and efforts, there will always be a residual number of flaws in their software. Yet only a small percentage of vendors currently participate in bug bounty programs, leaving a wide divergence between the security haves and have-nots.

The economics for startups and open-source vendors make large scale bounty programs and bounties a challenging prospect. Yet their revenue does not necessarily reflect how critical their software is, or the risks associated with it being exploited. Without industry-wide coverage across the software attack surface, end users are exposed.

3.5. Additional benefit: Depleting vulnerability stockpiles

The longer a given vulnerability exists, the more likely that it is rediscovered and exploited by other actors (vulnerability rediscovery, see box above), including criminals and nation-state adversaries. A bug bounty program reporting vulnerabilities to the vendor is an effective means to deplete the hidden stocks of zero-days exploits.

Research found a considerable rediscovery rate of vulnerabilities. For Android, 13.9% of vulnerabilities are rediscovered within 60 days, rising to 20% within 90 days and for the Chrome browser they found 12.57% rediscovery within 60 days [25]. Google's Project-Zero already invests in discovering and disclosing zero-day vulnerabilities and has shown this to be an effective method to ensure that the vulnerabilities it discovers are promptly patched by software vendors. Greater sharing of zero-days increases accountability of vendors to mitigate and secure software against all actors.

VULNERABILITY REDISCOVERY

refers to the likelihood of multiple parties discovering the same vulnerability independently of one another [26]. In the case of a nation state, **a zero-day exploit becomes worthless** if another party, for example the vendor in question or an independent researcher **disclose the vulnerability publicly**.

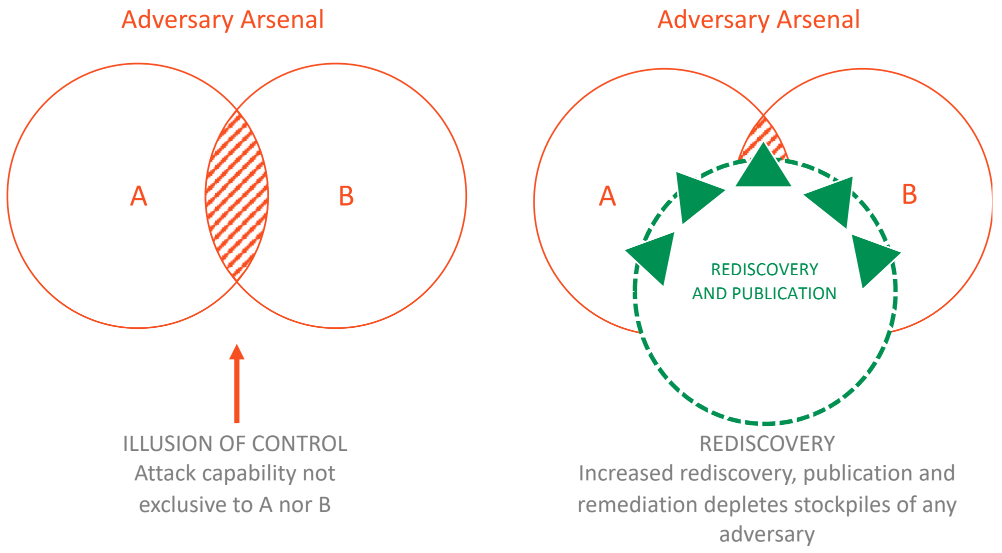

Adversary Arsenal
A
B
ILLUSION OF CONTROL
Attack capability not exclusive to A nor B
Adversary Arsenal
A
B
REDISCOVERY AND PUBLICATION
REDISCOVERY
Increased rediscovery, publication and remediation depletes stockpiles of any adversary

Figure 4 - Increased vulnerability research through a proposed bug bounty of last resort leads to increased independent rediscovery and publication of vulnerabilities stockpiled by criminals and nation state actors. Increased rediscovery is effective to expose vulnerabilities we cannot complete directly on price.

Creating and increasing incentives for tools and techniques that support vulnerability discovery (e.g., through bug bounty) is an effective method to drain the stockpile of offensive zero-day vulnerabilities [26]. Increased rediscovery of vulnerabilities systematically depletes the hidden arsenals of all actors (including actors that cannot be outbid on vulnerability price) - increasing overall security of the digital societies.

4. Conclusions

Our research and data show that existing Bug Bounty programs are successfully used to incentivize, formalize and strategically focus vulnerability discovery and research. Furthermore, we have demonstrated that the costs involved are trivial compared to the larger vendors revenue, and especially in comparison with industries that have similar security and safety requirements.

But we also discovered that to achieve industry-wide coverage more generally across the broader software attack surface, especially for financially and resource constrained software developers, will require the implementation of regulatory standards and collective investment.

We argue that industry-wide coverage of software vulnerabilities can be achieved by creating a Bug Bounty Program of Last Resort.

In summary, the main benefits of a Bounty Program of last Resort are:

- More effective collective and proactive cyber defense through faster and more efficient vulnerability discovery and remediation
- Transparency and internalization of costs - shifting the costs from end users and implementers to producers and vendors. Increased transparency into the security of software vendors
- A broad vulnerability safety-net for safe and secure innovation and rapid societal digital transformation. Including critical and prevalent open-source projects
- Systematically depleting nation state zero-day exploit arsenals

Society and businesses need to have assurance that they can safely and securely navigate the digital transformation. Our proposed solution provides this assurance and trust in the security of the software they deploy. It also enables emerging technology vendors and developers to focus on innovation first, without trading agility for security.

4.1. The authors

Oliver Rochford @OliverRochford works for Brim Security. Oliver is also advisor for Dark Defense AI GmbH, Picus Security, Adversa AI and CyberPal. Oliver has worked in security for over 20 years, and his past employers include Gartner, Tenable, and Qualys and Secunia.

Stefan Frei @Stefan_Frei works for SDX Security and teaches Cyber Security at ETH Zurich. Stefan has worked in security for over 20 years, and his past employers include Accenture Security, Swisscom, NSS Labs, Secunia, and ISS X-Force.

4.2. Acknowledgments

We thank for their contributions, review and input for this paper

- Aditya Kuppa
- Bernhard Plattner
- Didier Sornette
- Francisco Artes
- Lamine Aouad
- Pascal Gujer

Frontpage graphic designed by starline / Freepik

5. Future areas of research

Operating and Funding a Bug Bounty of Last Resort

This paper is focused on the economic argument for a BBPLR, and so we do not discuss implementation in detail, which remains for future research.

Several major questions remain to be addressed:

1. Who would run a BBPLR?
2. How would it be enforced?
3. How would it be funded?
4. How would we measure success?

In our future research we will review existing Bug Bounty models and approaches, as well as lessons learned for operational and funding models. We will also investigate existing Bug Bounty programs, for example the Internet Bug Bounty [23][24], and their impact - what works well, what doesn't - and how the model can be scaled up and optimized for broader adoption.

Lastly, we plan to conduct a review of prospective operational and funding models analogous programs in other industries, for example:

1. A national or regional agency approach, where a government or union agency is responsible for operating and enforcing the program. Funding could be from an agency or governmental budget.
2. An industry Association approach, where an existing or newly created industry association operates the program for a group of vendors. This could be funded through member contributions, in the form of insurance, or via governmental funding calculated on industry tax contributions. Without regulatory mandatory participation, this would likely result in weak participation and enforcement.

6. Further reading

- International Vulnerability Purchase Program (IVPP)
  https://techzoom.net/whitepaper/international-bug-bounty-progam
- Tenable: How lucrative are vulnerabilities?
  https://www.sciencedirect.com/science/article/abs/pii/S1361372319301241
- Cyber Resilience - Playbook for Public- Private Collaboration / WEF
  https://www.weforum.org/reports/cyber-resilience-playbook-for-public-private-collaboration

7. Bibliography

[1] NVD, "National Vulnerability Database," NIST, 2020. [Online]. Available: https://nvd.nist.gov.

[2] R. Lemos, "Special Report: National Vulnerability Database Analysis," 15 10 2020. [Online]. Available: https://techbeacon.com/security/special-report-national-vulnerability-database-analysis.

[3] J. Chong, "Bad Code: Should Software Makers Pay?," 03 10 2013. [Online]. Available: https://newrepublic.com/article/114973/bad-code-should-software-makers-pay-part-1.

[4] Accenture, "The cost of cybercrime study," Accenture Security, 2019. [Online]. Available: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf.

[5] NCSC, "Coordinated Vulnerability Disclosure: The Guideline," National Cyber Security Centre (NCSC), 10 2018. [Online]. Available: https://www.enisa.europa.eu/news/member-states/WEB_115207_BrochureNCSC_EN_A4.pdf.

[6] Attrition.org, "Legal Threats Against Security Researchers," 09 2020. [Online]. Available: http://attrition.org/errata/legal_threats/.

[7] K. Moussouris, "Data Security and Bug Bounty Programs: Lessons Learned from the Uber Breach and Security Researchers," 06 02 2018. [Online]. Available: https://www.commerce.senate.gov/services/files/E162FD54-F858-44AE-B25F-64E331C628AE.

[8] Miguel, "The 2020 Hacker Report," 2020. [Online]. Available: https://www.hackerone.com/sites/default/files/2020-10/the-2020-hacker-report%20%281%29.pdf.

[9] US-DOD, "Air Force Issues Challenge to “Hack the Air Force”," 26 04 2017. [Online]. Available: https://www.defense.gov/Newsroom/Releases/Release/Article/1164012/air-force-issues-challenge-to-hack-the-air-force/.

[10] HackerOne, "AIM HIGH...FIND, FIX, WIN!," 10 08 2017. [Online]. Available: https://www.hackerone.com/blog/hack-the-air-force-results.

[11] D. Fisher, "Researchers Find Bug Bounty Programs Pay Economic Rewards," 10 07 2013. [Online]. Available: https://threatpost.com/researchers-find-bug-bounty-programs-pay-economic-rewards/101243/.

[12] M. Finifter, "An Empirical Study of Vulnerability Rewards Programs," 14 08 2013. [Online]. Available: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf.

[13] "Shellshock (software bug)," Wikipedia, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Shellshock_%28software_bug%29.

[14] E. Silfversten, "Economics of Vulnerability Disclosure," 14 12 2018. [Online]. Available: https://www.rand.org/pubs/external_publications/EP67755.html.

[15] J. Vijayan, "More Attackers Have Begun Using Zero-Day Exploits," 04 06 2020. [Online]. Available: https://www.darkreading.com/attacks-breaches/more-attackers-have-begun-using-zero-day-exploits-/d/d-id/1337493.

[16] Zerodium, "We are Zerodium," 2020. [Online]. Available: https://www.zerodium.com.

[17] O. Rochford, "Tenable: How lucrative are vulnerabilities?," Tenable, 12 2019. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1361372319301241.

[18] D. Childs, "Pwn Tokio - Day Three Results," ZeroDayInitiative, 08 11 2020. [Online]. Available: https://www.thezdi.com/blog/2020/11/8/pwn2own-tokyo-live-from-toronto-day-three-results-and-master-of-pwn.

[19] S. Frei, "The Known Unknowns in Cyber Security," 05 12 2013. [Online]. Available: https://techzoom.net/whitepaper/the-known-unknowns-in-cyber-security/.

[20] S. Morgan, "2017 Cybercrime Report," Cybersecurity Ventures, 10 2017. [Online]. Available: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf.

[21] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," Wired, 22 08 2018. [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[22] NVD, "Common Vulnerability Scoring System (CVSS)," NIST, 2020. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss.

[23] D. Geer, "Cybersecurity as Realpolitik," BlackHat, 06 08 2014. [Online]. Available: http://geer.tinho.net/geer.blackhat.6viii14.txt.

[24] K. Costello, "Gartner Says Worldwide IT Spending to Grow 4% in 2021," Gartner, 20 10 2020. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2020-10-20-gartner-says-worldwide-it-spending-to-grow-4-percent-in-2021.

[25] CSIS, "The Economic Impact of Cybercrime and Cyber Espionage," CSIS, 22 07 2013. [Online]. Available: http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

[26] I. B. Bounty, "Internet Bug Bounty," 2020. [Online]. Available: https://internetbugbounty.org.

[27] D. B. Johnson, "SolarWinds, top executives hit with class action lawsuit over Orion software breach," SC Magazine, 04 01 2021. [Online]. Available: https://www.scmagazine.com/home/solarwinds-hack/solarwinds-top-executives-hit-with-class-action-lawsuit-over-orion-software-breach/.

[28] T. Herr, "Taking Stock: Estimating Vulnerability Rediscovery," Hoover Institution at Stanford University, 28 10 2017. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2928758.

[29] HackerOne, "The Wolves of Vuln Street," 15 04 2015. [Online]. Available: https://www.hackerone.com/blog/the-wolves-of-vuln-street.

[30] CVE, "Common Vulnerabilities and Exposures (CVE)," MITRE, 2020. [Online]. Available: https://cve.mitre.org/about/index.html.

[31] T. Robinson, "Flaws in open source library used by DoD, IC for satellite imagery could lead to system takeovers," SC Magazine, 29 01 2021. [Online]. Available: https://www.scmagazine.com/home/security-news/vulnerabilities/flaws-in-open-source-library-used-by-dod-ic-for-satellite-imagery-could-lead-to-system-takeovers/.

[32] Z. Zorz, "Sudo vulnerability allows attackers to gain root privileges on Linux systems," HelpNetSecurity, 27 01 2021. [Online]. Available: https://www.helpnetsecurity.com/2021/01/27/cve-2021-3156/.

[33] C. Cimpanu, "Backdoor code found in popular Bootstrap-Sass Ruby library," ZDNet, 15 04 2019. [Online]. Available: https://www.zdnet.com/article/backdoor-code-found-in-popular-bootstrap-sass-ruby-library/.

[34] S. M. Kerner, "Node.js Event-Stream Hack Exposes Supply Chain Security Risks," eWeek, 27 11 2018. [Online]. Available: https://www.eweek.com/security/node.js-event-stream-hack-exposes-supply-chain-security-risks.

[35] R. Chirgwin, "Have you updated your Electron app? We hope so. There was a bad code-injection bug in it," TheRegister, 14 05 2018. [Online]. Available: https://www.theregister.com/2018/05/14/electron_xss_vulnerability_cve_2018_1000136/.

[36] J. Wolff, "What Heartbleed Taught the Tech World," Slate, 22 10 2019. [Online]. Available: https://slate.com/technology/2019/10/heartbleed-lessons-open-source-code.html.

[37] M. Held, "The auto industry's growing recall problem—and how to fix it," AlixPartners, 01 2018. [Online]. Available: https://www.alixpartners.com/media/14438/ap_auto_industry_recall_problem_jan_2018.pdf.

8. Appendix

8.1. Data source: Vulnerabilities

This report relies on data from NVD, the US government's standards-based repository of vulnerability data [1]. Vulnerabilities that do not have a Common Vulnerability Enumeration (CVE) identifier are not part of the analysis [27]. Note that there are known issues with the National Vulnerability Database, e.g., delays in publication, and not all vulnerabilities industry-wide are included [2].

- The complete **NVD database** was retrieved on Jan 4th, 2020 from https://nvd.nist.gov/vuln/data-feeds

8.2. Date source: Financial Data

We used the revenue that the vendor earned over the trailing 12 months (TTM) for publicly traded companies, as reported by https://finance.yahoo.com on Jan 9th, 2021. Further sources are:

- **Red Hat** (acquired by IBM in 2018) https://craft.co/red-hat/revenue
- **Git Lab** (has plans to go public in 2021) https://getlatka.com/companies/gitlab
- **Huawei** (annual report 2019) https://www.huawei.com/en/annual-report/2019
- **Mozilla Foundation** (annual report 2019) https://assets.mozilla.net/annualreport/2019/mozilla-fdn-2019-short-form-0926.pdf
- **Canonical** https://www.phoronix.com/scan.php?page=news_item&px=Canonical-Report-FY2019

8.3. Data source: Bug bounty programs

Sources for bug bounty and security vulnerability disclosure programs:

- **Crowdsourced list of Bug Bounty programs** https://www.bugcrowd.com/bug-bounty-list/
- **Internet Bug Bounty** https://internetbugbounty.org
- **ZeroDayInitiative** https://www.zerodayinitiative.com
- **BugCrowd Programs** https://bugcrowd.com/programs
- **HackerOne Programs** https://hackerone.com/directory/programs
- **Safe Harbor Project** https://disclose.io

8.4. Software supply chain

Examples of recent vulnerabilities found in open-source projects and libraries. Some of these vulnerabilities remained undiscovered (by the public and vendor) for decades. These libraries or tools are a critical component of numerous downstream software products and services of many commercial vendors or service providers. Critical open-source code needs stronger institutional support for security, rather than just relying on volunteer efforts to find vulnerabilities. See also *Collaborating to Improve Open Source Security* [4]

Date	Vulnerability
Jan 2021	Flaws in open-source library used by DoD, IC for satellite imagery could lead to system takeovers [28].
Jan 2021	A vulnerability in sudo, a powerful and near-ubiquitous open-source utility used on major Linux and Unix-like operating systems, allows unprivileged local user to gain administrative privileges on host (CVE-2021-3156). Vulnerability hidden for about 10 years [29].
Apr 2019	Backdoor code found in popular Bootstrap-Sass library, a library with millions of users. Backdoor identified and within 8 days [30].
Nov 2018	Widely deployed open-source Node.js programming language module event-stream had been injected with malicious code [31].
May 2018	Vulnerability in Electron, a widely used desktop application framework, can be used to import arbitrary code (CVE-2018-1000136) [32]. Hundreds of desktop apps are based on Electron.[5]
Sep 2014	Shellshock is a family of security vulnerabilities in the Unix Bash shell that could enable an attacker to execute arbitrary commands and gain unauthorized access (CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187) [33]. Vulnerability introduced in 1989, hidden for 25 years. Within an hour of the publication there were reports of machines being compromised by the bug.
Apr 2014	The Heartbleed vulnerability caused by flaw in OpenSSL, a widely used open-source code library that implemented crypto protocols (CVE-2014-0160). Hidden for 5 years [34].

[4] https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/18542/2020_USA20_KEY-F02S_01_Collaborating-to-Improve-Open-Source-Security-How-the-Ecosystem-Is-Stepping-Up.pdf

[5] https://www.electronjs.org/apps

8.5. Glossar / Definitions / Concepts

BBPLR

Bug Bounty Program of Last Resort

VULNERABILITY REDISCOVERY

The likelihood that two or more security researchers **identify a vulnerability independently from each other**, also referred to as the collision rate. The threat of another security researcher or malicious actor rediscovering a vulnerability may serve as an incentive for vendors to patch the vulnerability as soon as possible.

VULNERABILITY DENSITY

Are vulnerabilities sparse or dense?

- If they are sparse, then every vulnerability you find and fix meaningfully lowers the number of vulnerabilities that are extant.
- If they are dense, then finding and fixing one more is essentially irrelevant to security and a waste of the resources spent finding it

We believe that vulnerabilities are sparse enough for a bug bounty of last resort to be effective. The growth of bug bounties witnessed over the past 10 years demonstrates the effectiveness of bug bounties [21].

CVE

Common Vulnerabilities and Exposures (CVE) is a a standardized name/identification for vulnerabilities and other information related to security exposures. CVEs help identify and correlate vulnerability information across products and services [27].

CVD

Coordinated Vulnerability Disclosure (CVD) process to coordinate the remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s) [5].

NVD

National Vulnerability Database (NVD) is a comprehensive database of reported known vulnerabilities which are assigned CVEs. It's operated by the National Institute of Standards and Technology (NIST). [1]

VENDOR

The term **vendor** is used to refer to the **producer of software**, regardless of whether or not that software is sold commercially

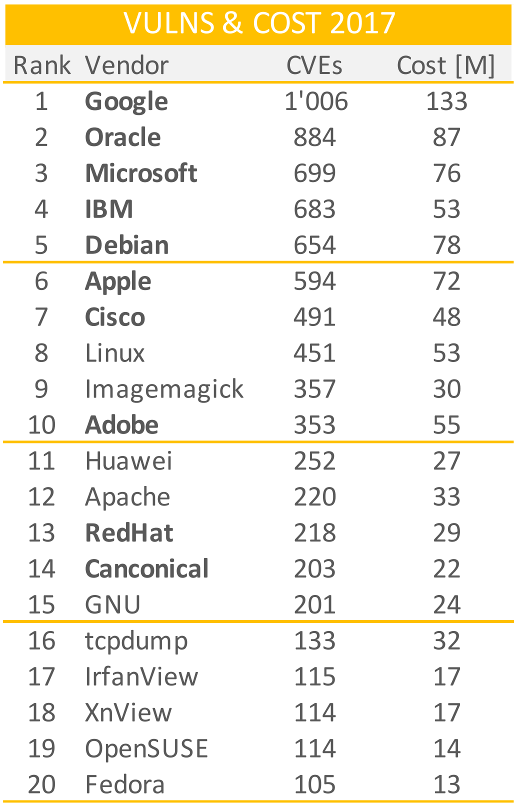
SECURE SDLC

Secure Software Development Life Cycle (SDLC) - A software development life cycle (SDLC) is a framework for building a software application from the design phase through to decommissioning.

8.6. Top-20 Vendors 2017 - 2018

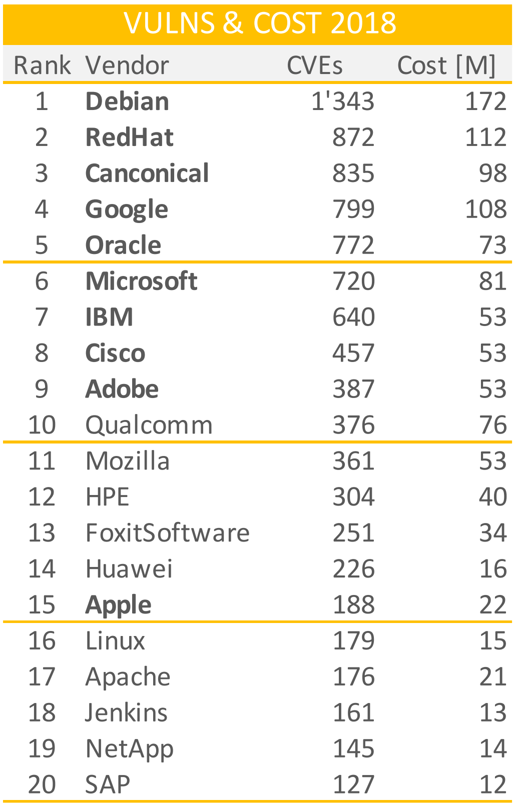
List of the top 20 vendors with the highest volume of vulnerabilities disclosed in 2017 and 2018.

- Cost in million USD to purchase the vendors vulnerabilities for USD 250k (critical), 150k (high) and 50k (medium) severity as of the model.
- Vendors marked in bold always were in the Top-20 from 2017 to 2020



VULNS & COST 2017

Rank	Vendor	CVEs	Cost [M]
1	**Google**	1'006	133
2	**Oracle**	884	87
3	**Microsoft**	699	76
4	**IBM**	683	53
5	**Debian**	654	78
6	**Apple**	594	72
7	**Cisco**	491	48
8	Linux	451	53
9	Imagemagick	357	30
10	**Adobe**	353	55
11	Huawei	252	27
12	Apache	220	33
13	**RedHat**	218	29
14	**Canconical**	203	22
15	GNU	201	24
16	tcpdump	133	32
17	IrfanView	115	17
18	XnView	114	17
19	OpenSUSE	114	14
20	Fedora	105	13



VULNS & COST 2018

Rank	Vendor	CVEs	Cost [M]
1	**Debian**	1'343	172
2	**RedHat**	872	112
3	**Canconical**	835	98
4	**Google**	799	108
5	**Oracle**	772	73
6	**Microsoft**	720	81
7	**IBM**	640	53
8	**Cisco**	457	53
9	**Adobe**	387	53
10	Qualcomm	376	76
11	Mozilla	361	53
12	HPE	304	40
13	FoxitSoftware	251	34
14	Huawei	226	16
15	**Apple**	188	22
16	Linux	179	15
17	Apache	176	21
18	Jenkins	161	13
19	NetApp	145	14
20	SAP	127	12

8.7. Top-20 Vendors 2019 - 2020

List of the top 20 vendors with the highest volume of vulnerabilities disclosed in 2019 and 2020.

- Cost in million USD to purchase the vendors vulnerabilities for USD 250k (critical), 150k (high) and 50k (medium) severity as of the model.
- Vendors marked in bold always were in the Top-20 from 2017 to 2020

VULNS & COST 2019			
Rank	Vendor	CVEs	Cost [M]
1	**Google**	874	90
2	**Microsoft**	848	99
3	**Debian**	730	93
4	**Oracle**	653	56
5	**Adobe**	569	92
6	**Cisco**	560	59
7	**RedHat**	556	64
8	**Apple**	538	66
9	**IBM**	473	39
10	Fedora	389	46
11	**Canconical**	357	43
12	OpenSUSE	347	41
13	Jenkins	344	33
14	CPanel	321	22
15	Qualcomm	298	47
16	Linux	292	29
17	Intel	236	21
18	FoxitSoftware	176	24
19	HPE	174	25
20	NetApp	171	20

VULNS & COST 2020			
Rank	Vendor	CVEs	Cost [M]
1	**Microsoft**	1'272	159
2	**Google**	1'215	143
3	**Oracle**	819	71
4	Netgear	606	61
5	**Cisco**	568	63
6	**IBM**	565	50
7	**Apple**	468	55
8	**Adobe**	313	43
9	Qualcomm	307	53
10	**RedHat**	306	30
11	**Debian**	271	28
12	OpenSUSE	249	27
13	Intel	240	24
14	GitLab	240	21
15	Jenkins	230	17
16	SAP	222	20
17	Fedora	219	22
18	Huawei	190	16
19	Mozilla	179	19
20	**Canconical**	162	13