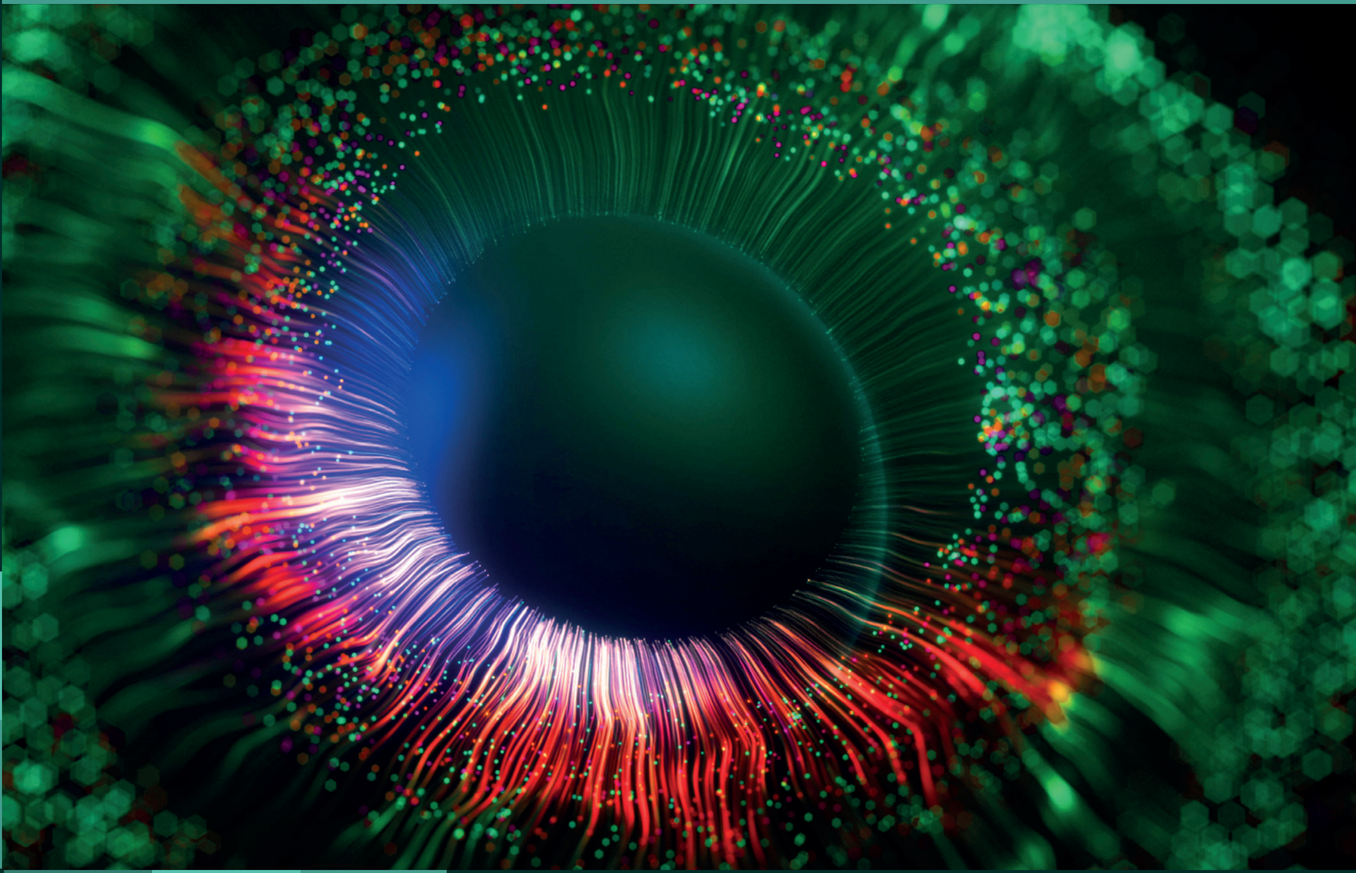
IoT Security Foundation

The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2022

A report prepared by Copper Horse Ltd

Published January 2023



Authors

Rohan Panesar, Mark Neve & David Rogers

Supported by

hackerone

Contents

Introduction

This is the fifth report in the series which plots the use of vulnerability disclosure in consumer markets with the introduction of enterprise starting in 2021. For consumers, knowing that a manufacturer has the requisite systems in place to receive, and remedy, known security flaws is a welcome form of assurance. Indeed, we have said many times that the lack of an easily identifiable method for reporting security issues could be likened to a canary in the coal mine – it's a good health indicator as to how serious they are about security.

Once again, we are delighted to partner with Copper Horse to produce and publish this report. They are experts in the field and have also monitored the evolution of contemporary practice within each report – making it much more valuable for practitioners and stakeholders alike. This report is no different; we trust you'll find the talking points and discussion as insightful as ever as we continue to promote vulnerability management as a basic hygiene practice for any company producing connected (Internet of Things) products and our advocacy is now support by regulation in the UK. To help companies meet the requirements of the regulation, a best practice guide can be downloaded for free from the website https://www.iotsecurityfoundation.org/best-practice-guidelines/ and our on-demand webinar series can be viewed here: https://www.iotsecurityfoundation.org/manage-vulnerability-reports-webinar/

John Moor, Managing Director, IoT Security Foundation

Vulnerability disclosure is the process by which a security researcher can report a vulnerability they have found in a product or service to the relevant organisation. Companies can implement a Vulnerability Disclosure Policy (VDP) that outlines how a researcher should submit discovered security vulnerabilities and how they'll be handled by the organisation. Years of organic development led to international standards and the general adoption of Coordinated Vulnerability Disclosure (CVD) as the best way of doing things.

This report looks at hundreds of consumer and enterprise Internet of Things (IoT) device manufacturers and whether there is any way for security researchers to disclose security issues and vulnerabilities to them. It is supported by open datasets which Copper Horse has published on https://www.copperhorse.co.uk to be used by others who wish to perform similar research or to validate the findings.

Methodology

In 2018, we researched 330 connected device manufacturers, taken from top retailers from across the globe, by looking at the top 10 connected devices they sold.

With each year of research and analysis of this dataset, companies are, expectedly, lost from the list. This year saw 18 companies, active in 2021, stop selling connected devices or cease operation. To counteract this loss, using the same methodology as 2018, 34 new companies have been added to this dataset for the 2022 release, resulting in a net increase of 16 companies. This helps to reflect the general changes in the market.

The full dataset for this report is public as open data at copperhorse.co.uk.

In 2021, a list of companies that supply enterprise, or business-to-business (B2B) IoT devices, was added to this research. This list has been kept in its original state, separate from the core dataset. An additional two 'workplace' category companies have been incorporated into the core dataset, and the enterprise category will be further reviewed in the next release of this report.

Threshold Test

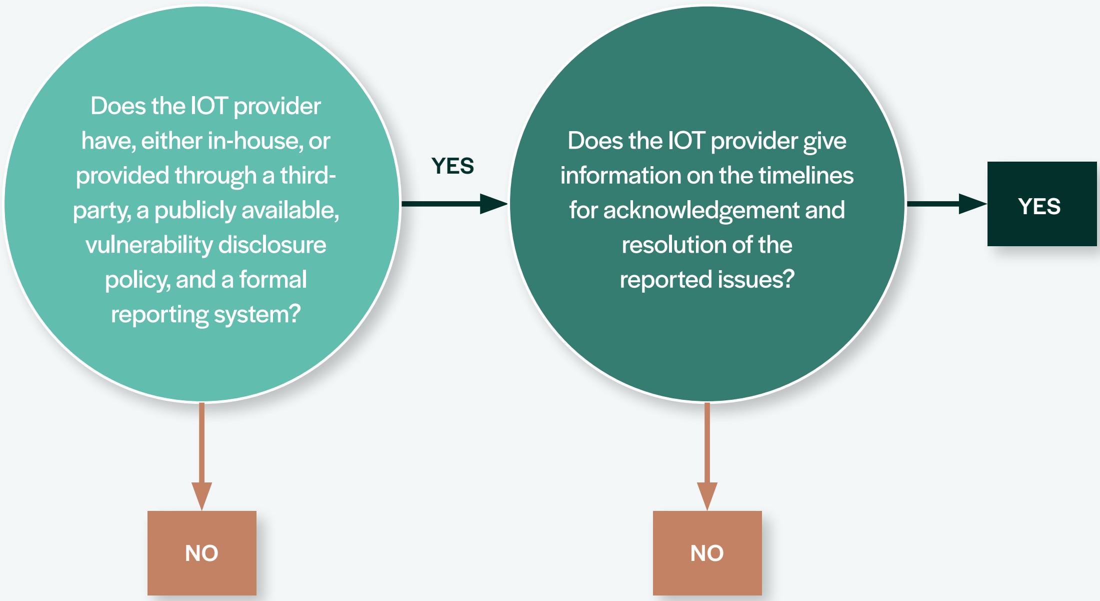

Does the IOT provider have, either in-house, or provided through a third-party, a publicly available, vulnerability disclosure policy, and a formal reporting system?
YES
Does the IOT provider give information on the timelines for acknowledgement and resolution of the reported issues?
YES
NO
NO

Figure 1

Of the 338 entries in the 2020 data, a staggering 274 would fail at the first hurdle. And of the 64 that meet basic threshold criteria, just 4 passed the second test.

Key findings

This research indicates that adoption of vulnerability disclosure, among the dataset, remains low. With more news of legislation and regulation around the world in this space, from countries such as the UK[1] and regions such as the EU[2] a large increase in adoption of CVD was expected.

With imminent legislation in the UK, we conducted a 'dip test' of popular devices sold by UK retailers in order to compare the data in this market and the review discovered that 70.59% (12/17) of the manufacturers of those devices have a vulnerability disclosure policy. 41.18% (7/17) of this cohort also included information about the timeline, and would be compliant with expected requirements. Timeline, in this context, refers to a policy indicating the expected response time from a manufacturer after initial contact by a security researcher.

Extrapolation based on current adoption rate

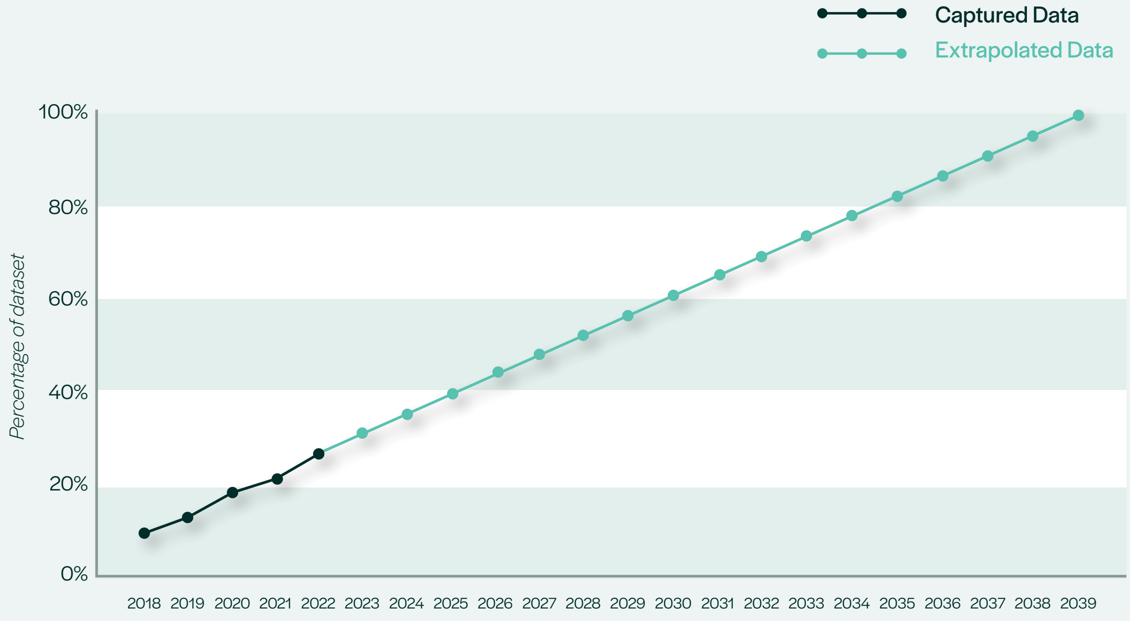
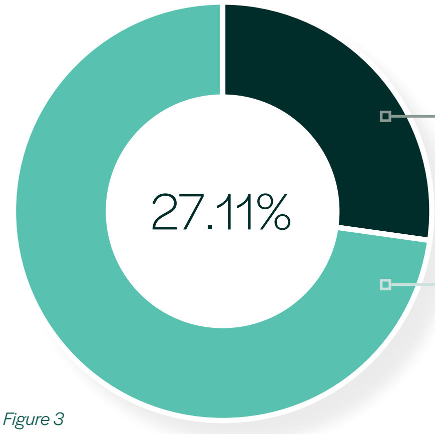


Figure 2

[1] https://bills.parliament.uk/bills/3069

[2] https://www.european-cyber-resilience-act.com

The Headline Figure



27.11% of the companies reviewed had a vulnerability disclosure policy

72.89% of the companies reviewed didn't have a vulnerability disclosure policy

Figure 3

In 2022, the data showed that 27.11% of the companies reviewed had a vulnerability disclosure policy. This is up from 21.6% in 2021, 18.9% in 2020, 13.3% in 2019, and 9.7% in 2018. The increase has been an average of approximately 4.3% each year. If this rate of adoption continues, 100% compliance will not be reached until 2039, shown in Figure 2 above. 27.11% represents only 90 of the total 332 companies reviewed, a net increase of 22 vendors (68 vendors with VDP in 2021).

Vulnerability Disclosure in Practice Trend

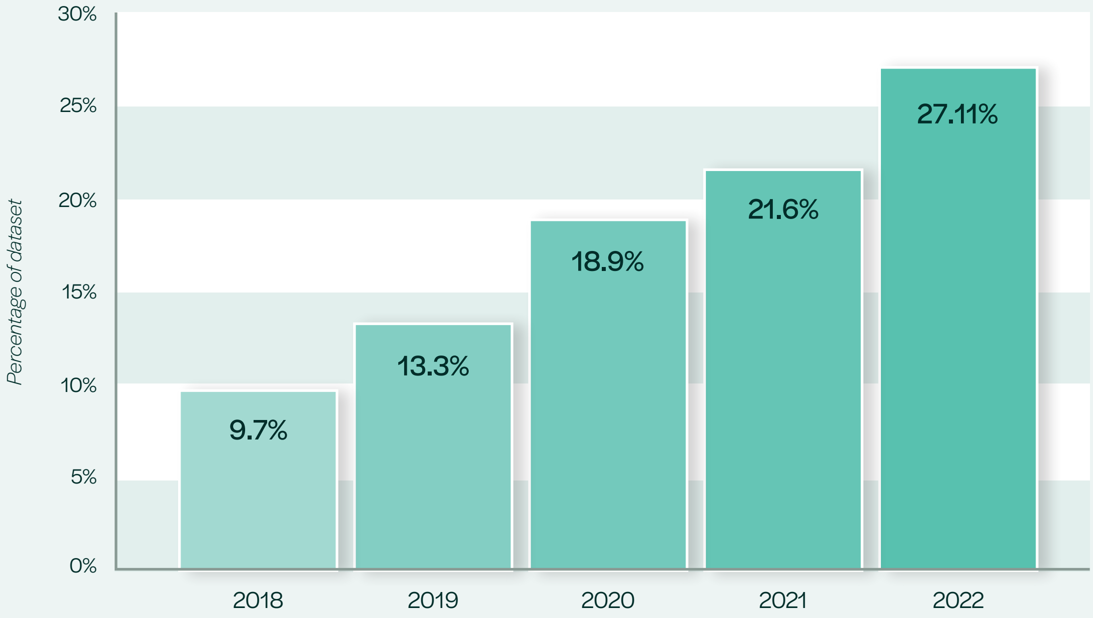


Figure 4

Crossing the Threshold

In 2020, a threshold test was introduced, pictured in Figure 1 to test the compliance of expected regulatory requirements. These being:

1. Have a vulnerability disclosure policy &;
2. Have some kind of information regarding expected timeline information.

Only 34 of the 332 vendors reviewed would pass the extended threshold test, equating to 10.24% of our dataset. While this is an increase on the 6.7% (21/68 of vendors with a detectable VDP) captured in 2021, the overall figure remains unacceptably low.

Secure Contact via PGP Falls

One of the biggest statistical changes, this year, has been in the PGP/GPG key area. This year saw 57.77% (52/90) offering contact using PGP. This an approximately 14% decrease on 2021's 71.8% (51/71). This may be due to more organisations using secure web forms for bug submissions, this is an area that may be reviewed further in a subsequent report.

Research Analysis and Developments

In 2022, the UK passed the Product Security and Telecommunications Infrastructure (PSTI) Act. The first part of the Act covers product security measures, including making it mandatory for manufacturers of consumer IoT products to implement a vulnerability disclosure policy. The threshold test in this report assesses the level of compliance of the organisations in the dataset with expected regulatory requirements, such as those enabled by the UK's PSTI Act. The first part of the test is the existence of a vulnerability disclosure policy, which 27.11% (90/332) of the dataset would pass. The second part covers the provision of expected timeline information by the manufacturer. Currently only 10.24% (34/332) of the companies in the dataset would pass the second test.

UK Retailer Compliance

We also reviewed the compliance of devices found at retailers selling in the UK. This was performed by looking at the popularity ranking of products at the major UK shops / online retailers, already used for this research. This included John Lewis, Currys, and Amazon UK. Of the popular devices sold by those retailers, 70.59% (12/17) of the manufacturers of those devices have a vulnerability disclosure policy. 41.18% (7/17) of this group also include information about the timeline and would be compliant with expected regulatory requirements. This contrasts with the wider picture of global manufacturers of 10.24% (34/332). While it is not possible to get exact retail data, it is possible to see the names of the manufacturers a retailer takes products from. This stocking choice by the retailer may reflect on the overall quality of the product offering and consequently (certainly in the future), on the manufacturer's approach to product security. The retail picture will be reviewed and expanded in future reports.

The difference between UK retailer and dataset figures

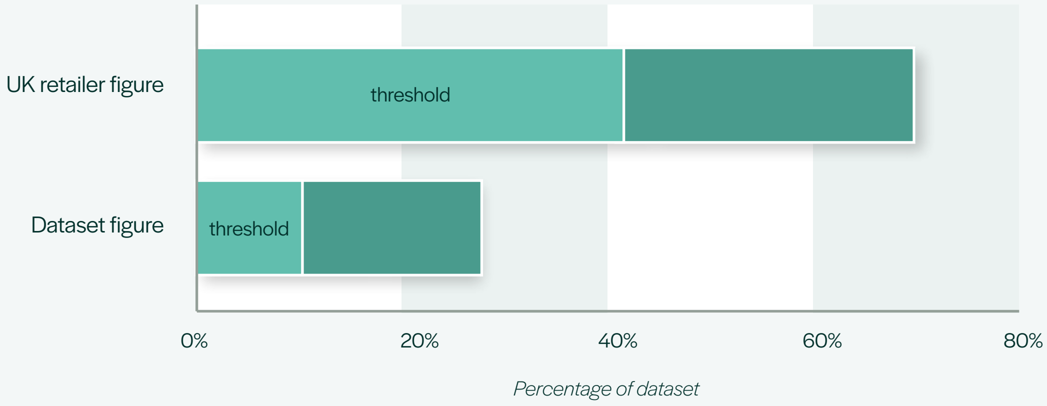


Figure 5

Types of Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) is the internationally standardised process via which a security researcher and vendor coordinate on identifying, rectifying, and eventually the disclosure plan of a discovered vulnerability. The CVD process ensures that a vulnerability is triaged properly, patched or fixed and the public is made aware[3]. Whilst CVD is the standardised and most well-understood method of disclosure policy, other ways of performing disclosures do exist. Often the disclosure type offered is not explicitly described in an organisation's Vulnerability Disclosure Policy (VDP). However, of the policies that do indicate a disclosure type, 68.88% (62/90) companies with a VDP have indicated that they operate Coordinated Vulnerability Disclosure. In the last report, 2021, this figure was 67.6% (46/68). Despite the benefits of CVD, 4 vendors have non-disclosure policies, where disclosure of a discovered vulnerability is not permitted (for unknown reasons). This is a slight decrease on the 5 companies with non-disclosure in 2021. The remaining companies with a VDP (24 of the 90) in the data, do not indicate one way or another what form of disclosure they support. Overall, the use of coordinated vulnerability disclosure is up and use of non-disclosure policies is down.

In 2022, the EU unveiled a new piece of draft legislation, the EU Cyber Resilience Act, in which they hope to improve the security of connected devices. One of the requirements for doing this is specifically mandating the use of Coordinated Vulnerability Disclosure[4]. Thus, 81.33% (270/332) companies in this data would be potentially non-compliant with this upcoming legislation, and of the companies currently engaging in vulnerability disclosure, 28/90 or 31.1% would still not be compliant, as they are not explicitly coordinated disclosure schemes.

Types of Vulnerability Disclosure

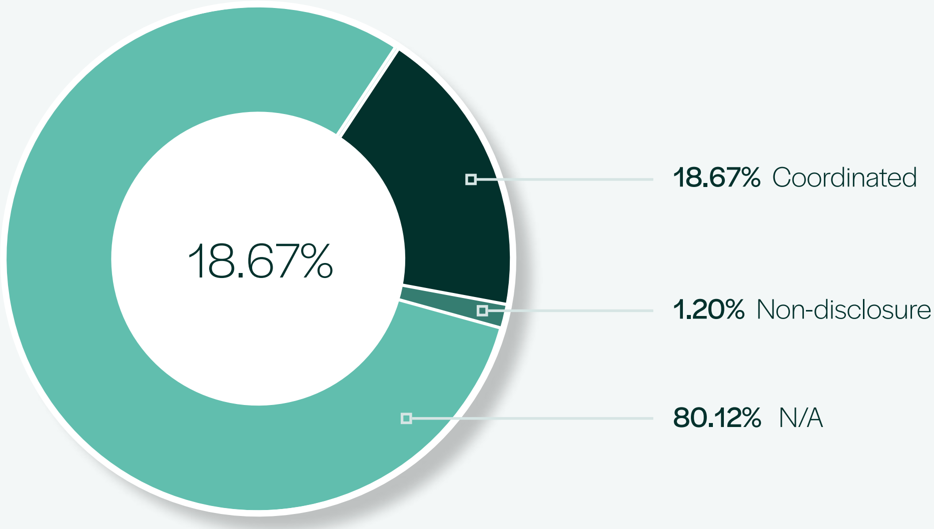


Figure 6

[3] https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu

[4] https://www.european-cyber-resilience-act.com/Cyber_Resilience_Act_Annex_1.html

Regional Differences

In terms of regional specific data, we have reviewed the dataset based on each vendor's headquarters location. In 2022 the situation has improved across all the regions captured in this data. Vendors with their headquarters in Asia have 34.69% (34/98), a rise from 29.5% (26/88) in 2021. Similarly, North America has also seen a marginal increase from 24.3% (35/144) in 2021, to 32.61% (45/138) in 2022. European vendors have, throughout the iterations of this report, lagged behind Asia and North America with vulnerability disclosure adoption. In 2022 it was observed that there was an increase in European vendors' adoption to 14.47% (11/76), from 9.0% (7/78) in 2021. With imminent legislation in Europe, it is surprising to see this gap not being reduced more.

Regional differences

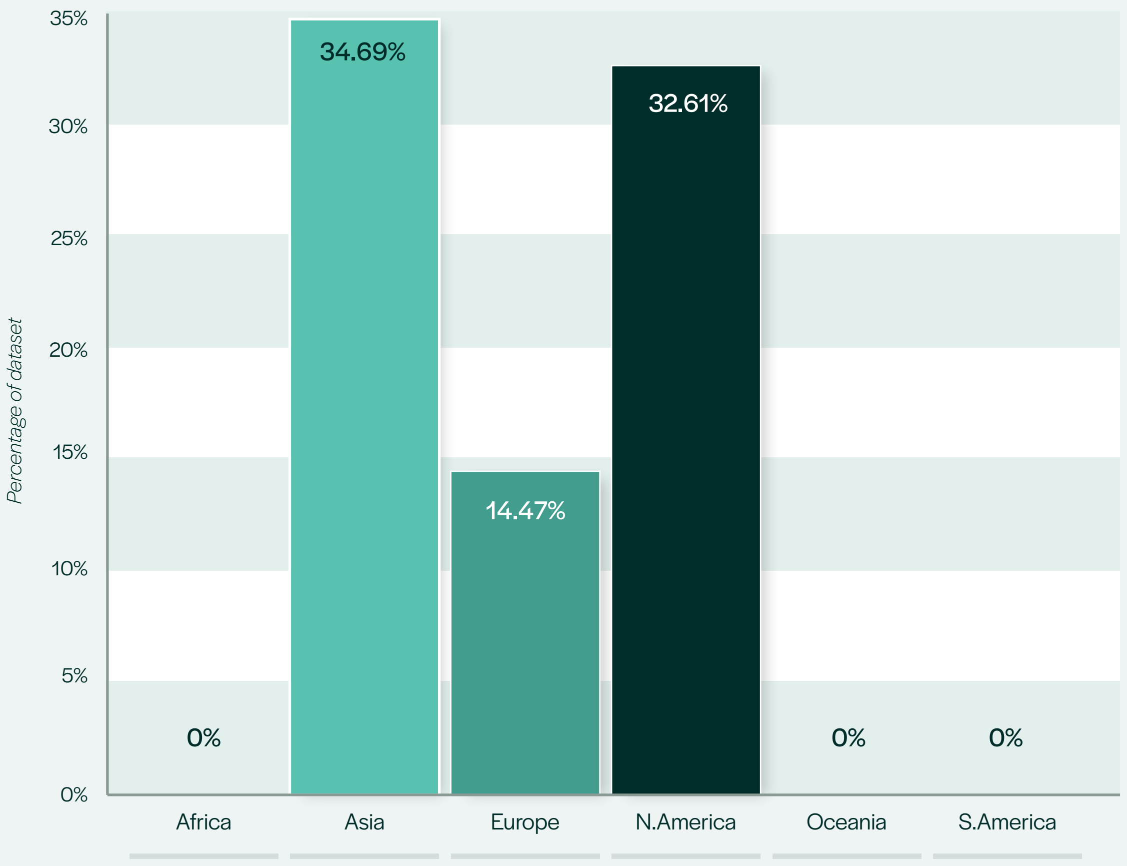


Figure 7

Product Categories

The trends observed throughout versions of this report are still apparent today. Well established, mature product categories trend towards higher adoption of vulnerability disclosure. The product categories: TV, Wi-Fi and Mobile are all well-established categories, with 100% (6/6), 84.62% (11/13), and 68.75% (11/16) adoption respectively. On the opposite end of the scale, some categories captured in this data have little to no vendors with a vulnerability disclosure policy. Leisure and Hobbies is at the far end with 0% of the companies within the category having a detectable policy. Following this is Health and Fitness with 10.53% (4/38), Environmental with 11.11% (2/18), and Lighting with 11.43% (4/35).

Percentage of Companies in a Segment with a Policy

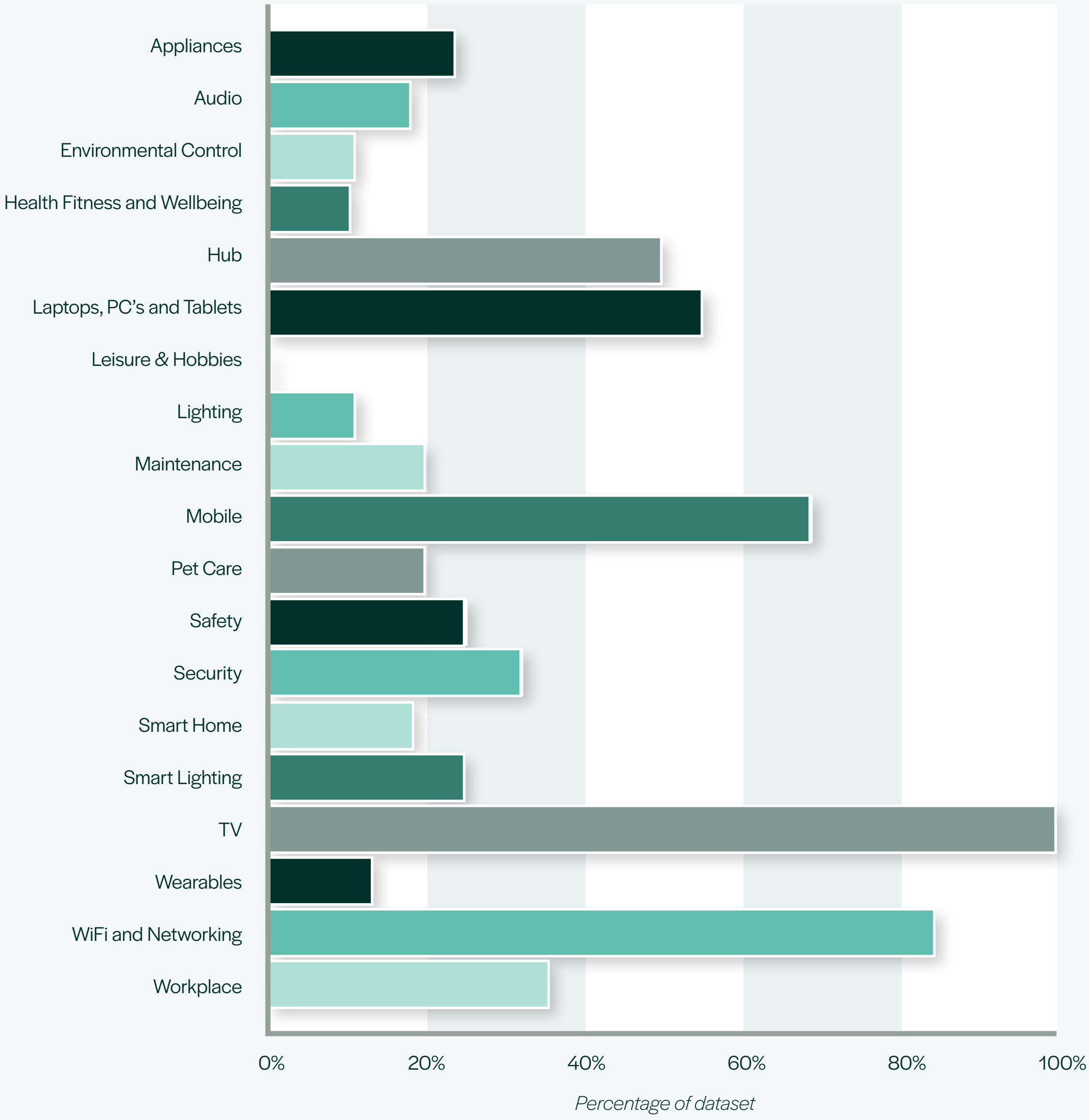


Figure 8

New additions to the 2022 report brought some interesting newcomers to product categories. Segway was added with their device the Ninebot, an internet connected one wheel transport device, in the Leisure and Hobbies category. BELLABEAT has been added to the Health, Fitness and Wellbeing category with their connected water bottle. This device has a partner app that helps users track their water intake. Neither of these newly added companies have a detectable vulnerability disclosure policy.

The 2021 report saw the Introduction of a set of Enterprise, or Business-to-Business (B2B) companies. This set of vendors has been kept separate to preserve the integrity of the original dataset, as this enterprise dataset was not obtained using the same methodology as the core data. This group of companies has seen a slight change, losing one company from the set, ‘ONI Vendor’, whose site would no longer load during the research phase. This year, 83.33% (40/48) of the enterprise vendors reviewed in this research had a vulnerability disclosure policy, in 2021 this figure was 71.4% (35/49). While this report isn’t a comprehensive study into the enterprise IoT landscape, it illustrates the huge difference in VDP adoption between consumer and enterprise IoT. This difference is potentially due to the maturity of the enterprise IoT sector, putting it in a better position than consumer IoT.

Proxy Disclosure and Bug Bounties

Bug bounties are a method for encouraging disclosure where security researchers are offered a financial incentive for the discovery and disclosure of vulnerabilities[5]. Research shows[6] that financial incentives are one of the greatest motivators for getting security researchers to participate in vulnerability disclosure. In our report, this year the research shows a slight increase on 2021 with 6.93% (23/332) offering bug bounty schemes versus last year's 6.67% (21/315).

This report also found that 6.33%, 21/332 (or 23.33% of companies with a VDP) of this dataset uses proxy disclosure, a modest increase on 5.1% (16/315) in 2021. Proxy disclosure is where a third-party organisation hosts and maintains a vendor's VDP. This research shows two proxy disclosure companies continue to dominate the third-party disclosure space, HackerOne and BugCrowd. These proxy disclosure organisations are proponents of vulnerability disclosure, not only hosting policies through their platforms but also engaging with the security researcher community. These organisations also educate security researchers and hackers, helping them to begin engaging with CVD. This is partially achieved by hosting conferences and events, and offering resources on their sites for budding security researchers.

In the 2021 report, Wink was captured as using proxy disclosure. When conducting the research in 2022, the company still has a HackerOne page but at the top it states "Wink is taking a break and is not accepting new submissions." The reason for this pause is unknown and not provided on Wink's site or proxy disclosure page.

[5] https://www.hackerone.com/vulnerability-management/what-are-bug-bounties-how-do-they-work-examples

[6] https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

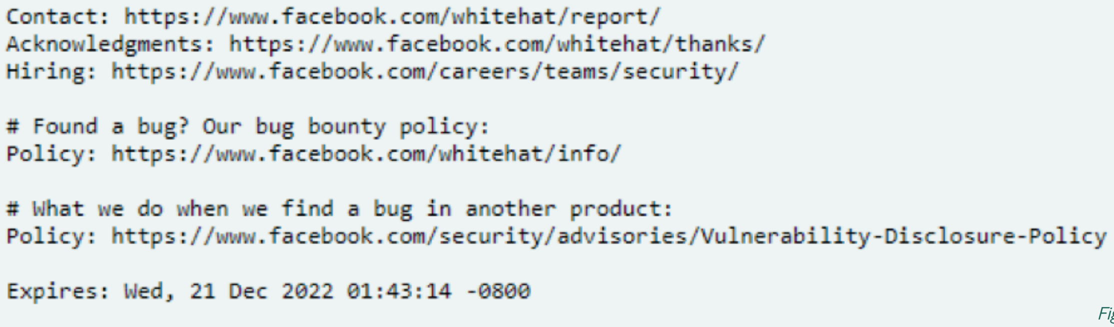
Use of /security

The ease with which a security researcher is able to find an organisation's policy directly relates to the researcher's ability to properly disclose vulnerabilities to the company. One location used to advertise a VDP is a '/security' page. 7.53% (25/332) of the vendors in this dataset utilise the /security page as the location of their VDP, or 27.77% (25/90) of the companies that have a VDP. This is a slight increase on the 5.4% (17/315) in 2021. While the overall percentage (7.53%) is not particularly large, over a quarter of the companies in this dataset with a vulnerability disclosure policy use /security to host their policy. The remainder of the companies in this dataset host their policies on other pages of their websites.

Use of security.txt

The UK's National Cyber Security Centre (NCSC) has developed a toolkit for implementing a vulnerability disclosure policy[7]. One of the recommendations in this toolkit is the use of security.txt. This is a standard, machine-readable location on websites for organisations to outline their disclosure policies[8]. This year, the number of companies using security.txt has increased to 5.72% (19/332) in 2022 from 2.9% (9/315).

Meta'/Facebook's security.txt Example



```
Contact: https://www.facebook.com/whitehat/report/
Acknowledgments: https://www.facebook.com/whitehat/thanks/
Hiring: https://www.facebook.com/careers/teams/security/

# Found a bug? Our bug bounty policy:
Policy: https://www.facebook.com/whitehat/info/

# What we do when we find a bug in another product:
Policy: https://www.facebook.com/security/advisories/Vulnerability-Disclosure-Policy

Expires: Wed, 21 Dec 2022 01:43:14 -0800
```

Figure 9

The image shown above is Meta'/Facebook's security.txt. One feature of this that is often overlooked, is the expiration date. This was first reviewed earlier in 2022 and had an expiration date of November 18, 2022. It appears Meta updates its security.txt monthly, as on upon later inspection, in November 2022, the expiration date had been updated to December 2022. A required element by the informational IETF RFC published in April 2022[9] indicates to a researcher whether the policy they are looking at is stale. It is recommended by IETF and security.txt that this is less than a year into the future so that researchers know that a policy is regularly maintained. The implications of an expired policy are discussed further in the Talking Points section of this document.

[7] https://www.ncsc.gov.uk/information/vulnerability-disclosure-toolkit
[8] https://securitytxt.org
[9] https://www.rfc-editor.org/rfc/rfc9116#name-expires

PGP Key

The use of PGP/GPG to secure submissions is included as an option element in the NCSC's vulnerability disclosure toolkit, and some vendors choose to include it in their policies. By providing a public encryption key, vendors can give confidence to researchers that they are interested in securing the information about the vulnerability that is being disclosed to them. In 2022, over half the companies researched that already had a VDP also have a PGP key researchers can use. This number is 57.77% (52/90), an approximately 14% decrease on 2021's 71.8% (51/71).

Companies No Longer Operating

With each iteration of this report, companies have been lost from the dataset. 2022 saw 18 companies removed from the list (21 in 2021), because they have either stopped selling connected devices, or because they have stopped operating entirely. While the reasons for a company ceasing operating is often impossible to glean, a loss of this number is not unexpected. The previous reports saw losses in similar areas. One area with observed losses each year, is 'generic smart devices', or what appear to be white label goods, often sold via Amazon or AliExpress, and spanning multiple product categories such as smart plugs and lightbulbs. These devices are often listed by sellers one year but then, the next year, these same sellers list completely different products. In one case in a previous report, research discovered a seller of IoT products switching to selling balloons the following year. In other cases, the sellers disappear from the retail platforms.

The COVID-19 pandemic is still causing issues for start-ups. SmartHalo, a start-up making smart devices for bicycles, posted on their Kickstarter page that they would have to stop operating. They indicated[10] that the pandemic and the difficulties making visits to component manufacturers in China due to closed borders caused them to run out of cash and eventually to stop operating.

When first conducting this research in 2022, it had recently been announced that Onkyo, the audio brand, had gone bankrupt. Upon later review of the data, a company had, in the interim, bought Onkyo and saved them from bankruptcy. The company was therefore retained in the data.

[10] https://www.kickstarter.com/projects/smarthalo/smarthalo-2-make-your-bike-smarter/posts/3361104

Talking Points

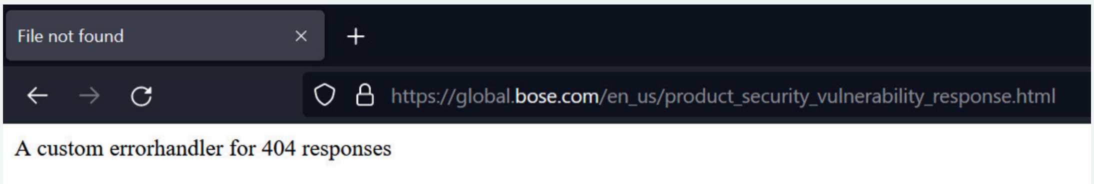
Over the multiple revisions of this report, one common observation has been expired or outdated vulnerability disclosure policies. When reviewing whether an organisation has a VDP, we often encounter policies in various states of abandonment. It is therefore difficult for a researcher to assess whether a policy is still maintained, without a distinct expiration date, until they try and make contact and potentially receive no reply.

One way this materialises in this research is outdated proxy disclosure pages. For example, Ecobee has a community-provided HackerOne page. This means the policy details have been added by a member of the HackerOne community. While it appears the Ecobee's policy is "Community Provided", there still exists a button to access bug submission form. This indicates there may have once been an Ecobee policy hosted on HackerOne. If a security researcher were to use this form to submit a critical, time sensitive vulnerability, it is unclear as to whether they would receive a response.

During the research phase of this report, FitBit was discovered to be in what seemed to be a transition period. FitBit previously had a BugCrowd page. BugCrowd even released an article announcing their partnership with FitBit[11] and FitBit used to have a /security page on their site pointing researchers to a dead proxy disclosure page. When reviewing the data for this report it was discovered that FitBit had been acquired by Google, and between the research and writing phases had updated their point of contact for submitting vulnerabilities to Google Bug Hunters. This change has not been made to the data of this report, as it happened outside the research window, but will be reflected in the 2023 report. Similarly, Procter & Gamble have a security.txt that indicates their policy was once hosted by HackerOne[12]. This policy is now registering as being community provided (usually indicating it has been added by a user of the proxy disclosure site) and an external policy to HackerOne, but the policy itself is still filled with references to HackerOne, including requiring a HackerOne email to take part.

Another example of expired vulnerability disclosure policies appears on the audio company Bose's website. When visiting Bose's /security page it returns a 404 error, but the URL indicates that there was once a VDP hosted at that location. While they do maintain a policy elsewhere, they have moved it from the /security page.

Bose's /security Page 404 Error



File not found
https://global.bose.com/en_us/product_security_vulnerability_response.html

A custom errorhandler for 404 responses

Figure 10

[11] https://www.bugcrowd.com/press-release/bugcrowd-launches-public-bug-bounty-program-for-fitbit/

[12] https://hackerone.com/proctergamble?type=team

TomTom previously had both a HackerOne posted proxy disclosure page as well as a policy available on their site, with a hall of fame for recognising the contributions of researchers. In 2022, it appears their policy has become obsolete. The HackerOne page has become “provided by a community member” and the policy on the TomTom site itself is nowhere to be found; links to the policy that previously functioned returned nothing. All that remains is the hall of fame from 2019 – with no new additions to it.

Implementing vulnerability disclosure as an organisation can be difficult. Creating a comprehensive scope and properly maintaining a programme can be complicated for a small-sized IoT manufacturer with one product, let alone one with many product divisions across a large number of product categories. Samsung hosts a site that points a researcher to the correct point of contact based on the device they are testing. Found at securityreport.samsung.com - security researchers can find a link to for the correct contact at different product divisions as well as Samsung’s overall policy easily accessible on the main site. This unified approach and experience makes the life of security researchers simple and exemplifies good practice – scaled up!

The overall picture for consumer IoT vulnerability disclosure remains disappointing as adoption levels by manufacturers are still very low. However, of those that do implement and manage programmes, some vendors go above and beyond, which is refreshing to see. While the lower end of the scale of vulnerability disclosure policies can lack clarity and cause confusion in the disclosure process, companies can add features, beyond what is recommended in standards and guidance, that improve the quality and potentially draw more researchers to a programme. In Meta/Facebook’s programme is the option to have a reward payment doubled if the researcher chooses to donate the pay-out to charity.

In the ENISA ‘Economics of Vulnerability Disclosure’ paper[13], the European agency outlined the main barriers for entry for security researchers participating in vulnerability disclosure. One of these is fear of legal consequences. For this reason organisations might use a legal safe harbour clause in their policy; essentially the vendor organisation gives a researcher consent to test their products[14]. A good example of this is LG’s policy where the company includes the text – “LGE does not take unreasonable punitive actions against security issue reporters, like making legal threats or referring matters to law enforcement.” Clauses like this give researchers the confidence and authority they need to test devices without the fear of repercussions.

Panasonic makes its policy incredibly easy for researchers to find. The company’s policy is available from a Google search as well as on its site. The company provides a vulnerability submission path, PGP key and the actual policy on all the relevant pages, which makes the submission process for a researcher smoother.

Apple has recently taken a more positive approach to CVD, where the company advise researchers how to maximise their pay-outs by targeting specific areas of interest. In October 2022, Apple announced it would be upgrading its bug bounty scheme[15]. Since the launch of the original programme in 2016, Apple claims to have paid out almost $20 million to researchers. The bug bounty upgrade has been made and appears to provide clarity for researchers and improve the efficiency of the vulnerability disclosure process. In the blog post announcing the upgrade to the programme, the company stated that they are improving the time it takes them to respond to bug reports, developing a new feature for the Apple Security Research site for easier submission of vulnerabilities with real time updates. Interestingly, in Apple’s bug reporting guidelines[16] the company outlines that their bounty pay-outs are not only based on the severity of the submitted vulnerabilities, but also based on the clarity provided by the researcher in terms of quality of the report, making it easier for the security team at Apple to reproduce the issue.

13. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

14. https://www.hackerone.com/vulnerability-management/attorneys-view-vulnerability-disclosure

15. https://security.apple.com/blog/apple-security-bounty-upgraded/

16. https://security.apple.com/bounty/guidelines/

Conclusions

The general story is depressingly similar to the previous annual reports published by the IoTSF. There is a small increase in companies using vulnerability disclosure, following the same growth path as the previous data. Just under three quarters of the IoT manufacturers studied have no way for security researchers to contact them. It appears that this rate of adoption is far too slow, even with the imminent threat of legislation and regulation. It should be noted however that this report does not cover market share and the companies listed as meeting the threshold tests for a detectable vulnerability disclosure policy represent significant global market share. This was reflected in the products on sale in one country, the UK, where the adherence to the vulnerability disclosure requirement of the country's new Product Security & Telecommunications Infrastructure (PSTI) Act was already high amongst the products stocked by major retailers.

Most of the other areas of data captured in this report have also seen slight improvements compared to the previous year, with one exception – the decrease in the provision of PGP keys as an offered method of securing communications between manufacturers and researchers. The suspicion in the Copper Horse team is that this may be a less preferred way of operating by companies and researchers and that the use of secured webforms and portals may provide alternatives to PGP or GPG. The team may investigate this further in next year's report.

A positive trend observed in this research is that the use of Coordinated Vulnerability Disclosure is on the rise, and the use of non-disclosure policies is decreasing.

Not all vulnerability disclosure policies are created equally. The talking points section of this report discussed how important language coherence and a lack of ambiguity are, when developing a vulnerability disclosure policy. Policies provided by community members of proxy disclosure sites and policies on manufacturer sites without expiration dates add to this lack of clarity. This will reduce the efficiency of the vulnerability disclosure process overall.

While the adoption figures for VDPs are still disappointingly low, vulnerability disclosure finally making its way into law will make next year's report a potential interesting turning point in the IoT security landscape.

What else?

Vulnerability management is a long-standing, necessary central process in security management. Looking ahead, we believe there is unrealised potential, which could be unlocked with better, smarter, automated systems.

As noise surrounding the recent OpenSSL vulnerability has shown[17],there is a clear need to automatically detect which connected systems are impacted by a disclosed vulnerability. In our journey towards a "continuous assurance" model, critical innovations in vulnerability management, software dependency disclosure (SBOM) and smarter networking, all have a role to play. We're working on this model with schemas created by industry partners within our ManySecured collaborative initiative – see manysecured.net

IoT Security Foundation

[17] https://manysecured.net/openssl/

Annex

Threshold Test 2

The 34 companies that would pass the first and second threshold test – that they have a detectable vulnerability disclosure policy and additionally provide timeline information, are listed below:

Anker, Eufy
Bosch
BroadLink
BT
Canon
Ecobee
Foscam
HMD Global (Nokia Mobile)
Huawei
June
Lenovo
LG
Logitech
Logitech, Ultimate Ears
Meta
Microsoft
OPPO
Panasonic
Peloton
Philips
Procter & Gamble, Oral B
Qnap
Quardio
Samsung (Smart TV)
Sengled
Siemens
SimpliSafe
SonicWall
Sonoff
Synology
TP-Link
Western Digital
Wink
Xiaomi (MI)

Threshold Test 1

The 56 companies that would only pass the first threshold test, the existence of a detectable vulnerability disclosure policy, are listed below:

Acer
Amazon
Apple
ARLO
Arris (Commscope)
ASUS
August
Belkin
Best Buy, Insignia
boAt
Bose
Buffalo
Canary
Dahua
Dell
Devolo
D-Link
Draytek
Eero
FLiR
Garmin
GE Appliances
Google
Hanwha, Wisenet
Hikvision
Honeywell Home (Resideo)
HP
HTC
JBL
Lexmark
Lifx
Linksys
Lovense
Motorola Mobility
Netgear
Nuki
OnePlus
PetCube
Ring
Roku
Samsung (Galaxy Watch)
Samsung (Mobile)
Samsung (SmartThings)
Schlage, Allegion
Signify - Philips Lighting
Sonos
Sony
Tapplock
TVT
Vivint
Vivo
WiZ (Signify)
WyzeCam
Yale
ZTE
ZyXEL

Annex (cont.)

No Discoverable Vulnerability Disclosure Policy

Listed below are the companies that do not pass threshold test 1 (no VDP policy at all):

116 Plus
ACEMAX
ACTi
AdhereTech
ADT
Aeon Labs, Aeotec
Airboxlab
Airthings
AISIRER
Aiwa
AKILII
AliveCor
Amaryllo
Amazfit (Huami)
Amor Gummiwaren GmbH
Anoto
Anova
ApnaCam
Apollo Tech USA
Apption Labs
Armani (Armani Exchange, Emporio Armani)
ASAKUKI
Atom Labs
Audio Pro
Awair
B&O
Bawoo
BeBird
Beeline
Behmor
BELLABEAT
Beurer
Bizfeat
BLU Products
BlueAir
Breathometer
Brother Industries, Ltd
Buddy
Candy
Canon, IRIS
Casio
Catapult Sports
Chamberlain
Circle
Clever Dog
Click and Grow
Curb
Current Labs
Deeper
Delta Five
DENON
Devialet
DigitalKeys
Doogee
Double Robotics
Drayton
Dyson
Edimax
EGLO
ELAiCE
Elecom
Elgato, Eve
Eminent
EMOOR
Enabot
Energenie
eq-3
Estimote
Etekcity
Eve
Expower
EZVIZ
F22
FIBARO
FireAngel
FitBit
Flux Smart
Fossil
FREDI
Furbo
Garadget
Gardena
Genetic International, Ultralink
Genius Hub
Gosund
Greater Goods
Guardian Technologies
Hangzhou XiongMai Technology
Hank
Hatch Baby
HAVIT
Haylou
HeimVision
Hidrate
Hoco
Hoover
Hunterfan
Husqvarna
Icontrol Networks Canada
iFAVINE
IFITech
IglooHome
iHealth
iku
ilumi
Infinix
Innr
Insteon
Intelbras
InteraXon Inc
Iris Ohyama
Jasco
Keen Home
KeySmart
Kickstart
Kidde
Kobo
Kolibree, Baracoda
Koogeek
Kwikset
Lampaous, LUMENMAX
Laurastar

Annex (cont.)

Lenbrook Industries, Bluesound
Leotec
LetsFit
LifeFitness
LIGE
Lightwave
Lithe
Lockstate, smartLOCK, RemoteLOCK
Lohas
Lorex
Loxone
Lutron
Marshall
Mattel, Fisher-Price
Mellow
Merkury Innovations
Meross
Michael Kors
MIPOW
Misfit
Moen
MoKo
Moleskine
MSI
MySpool
NAIM
NanoLeaf
Neato
Neo
Nespresso
Netatmo
Neurio, Generac
Night Owl
Nima
Noise
Nologie
NordicTrack
Novostella, Ustellar
Omron
ONKYO
Osram
Otio
Perfect Company
Pico
PicoBrew
Polar
Proform (ICON fitness)
Rachio
Ratoc Systems
Remotec
RENPHO
Reolink Digital Technology
Roberts Radio
Roost
Ruark
Sacramento
Segway
Seiko Epson
Seneye
Sensibo
Sensoria
Shenzhen Neo
Skybell
Sleep Number
Small
Smanos
Smarter Applications
SmartPlate
SmartyPans
Sphero
StoryLink
SUUNTO
Tado
Tado
Tanita
TCL Corporation (Alcatel)
Teckin
Tefal
Tend Insights
Theatro
TIBO
Tile
Tomshine
TomTom
Tracking Point
Trane
TRENDnet
Trust
TytoCare
Tzumi
UBTECH
Ustellar
Vankyo
Vaultek
Veho
Velco
Venturer (RCA)
Vivitar
Voxx International, Klipsch
Wallfire
Wattcost
Wearable X
Weber
Weenect
Weight Gurus (Greater Goods)
We-Vibe
Whirlpool
Whistle
Wimius
Winix America
Withings
XOLO
Xoopar
Xperi, DTS
X-Sense
Yamaha Pro Audio, Yamaha Corporation
Yeelight
YP
Zeeq
Zmodo Technology

IoT Security Foundation

www.iotsecurityfoundation.org

COPPER HORSE

www.copperhorse.co.uk

59-60 Thames Street, Windsor, Berkshire, UK, SL4 1TX
+44 (0) 208 1337 733 @copperhorseuk