IoT Security Foundation

# The State of Vulnerability Disclosure Policy (VDP) Usage in Global Consumer IoT in 2024

**A report prepared by Copper Horse Ltd**
**Published November 2024**


Authors

Mark Neve & David Rogers


*Supported by*

hackerone

# Contents

# Introduction

**Each year I look forward to reading the findings of this report and the commentary that augments it. It is a unique barometer of the progress that is being made in the global consumer IoT market, and in recent times can be compared to commercial products used in an enterprise setting.**

In April this year, we finally saw the UK's PSTI enactment after its progress was delayed due to the global pandemic. This report illustrates how we are seeing the effect, and intended outcomes of the UK regulation. It also shows those that are following in Europe and the US are consistent in pointing the way forward, not just regarding product security, but also the processes that are expected of the supply chain to ensure security is monitored and maintained throughout life usage.

Aside from the headline trend figure – which is encouraging - several sections caught my eye in particular in this report. The first was the retailer section which shows how the UK legislation has driven a bigger improvement than European and US retailers. Whilst the sample set maybe low, it is a consistent gauge moving faster in the right direction. Even John Lewis - whose stocked goods faired very highly at 90% in 2023 improved their position with only Smyths (UK) and Target (US) raising an eyebrow.

The second trend to note is the comparison and gap in practice between the consumer and enterprise sectors. Whilst the consumer sector is firmly heading in the right direction, there is a stark contrast in market practice levels and continues to justify the need for consumer regulation.

The third section relates to the relative positions of individual product categories with notable laggards being Health and Fitness, Lighting and, somewhat paradoxically, Security. Those manufacturer report cards read "must do better".

I conclude by observing the situation is improving but there is still a lot of room for improvement - in an increasingly digital world, without fit-for-purpose cybersecurity, we are all at risk.

Finally, I'd like to congratulate the Copper Horse team once again for diligently providing time-series documentary evidence that helps us understand the context and state of cybersecurity in connected (IoT) products on the market. I fully commend this report to the reader.

*John Moor, Managing Director, IoT Security Foundation*

This is the seventh report into the state of vulnerability disclosure practices by manufacturers in the IoT product ecosystem. This is the longest running and most stable tracking of what is a very basic public indicator of whether a company takes product security seriously. This indicator is a contact page for security researchers to use in order to report security vulnerabilities they have discovered to a company. If that contact point doesn't exist, it is extremely difficult for those issues to be reported from the 'good guys', whilst the 'bad guys' are never going to report anything – they'll exploit the vulnerabilities as much as they can for their own ends.

It can be very difficult to differentiate levels of security between physical products as it is hidden from inspection. This has allowed many companies in the past to ignore very basic product security measures such as leaving in hard-coded default passwords and the ability for easily accessible remote access. This in turn has left the door wide open for exploitation by different threat actors, ranging from nation states to ransomware criminals.

The concept of vulnerability disclosure is often misunderstood outside of the security and hacking world. It is repeatedly confused with the concept of incident reporting (or disclosure), where companies are required in some jurisdictions to alert the authorities of some kind of data breach or compromise. Vulnerability disclosure is specifically not that – it is about security researchers disclosing vulnerabilities to a company in order to get them rectified – to protect the company's products and services, but most importantly the company's customers. It is not about asking companies to disclose public information about unresolved vulnerabilities they may have. It is perhaps worth noting that a better nomenclature would help to resolve this misunderstanding in the future; this is some homework for the reader of this report!

The UK's Product Security and Telecommunications Infrastructure (PSTI) Act's regulations came into force on the 29th of April 2024, making it the first country in the world to demand vulnerability disclosure by IoT manufacturers of consumer products. It's relative equivalent in the EU, the Cyber Resilience Act (CRA), goes further and with some classes of product subjects them to more stringent requirements and conformity assessments. The finalisation of the CRA 2024 means that regulation comes into force from 2027.

In March 2024, the FCC in the USA introduced a 'Voluntary IoT Labeling Programme'[1] for wireless consumer IoT products, which builds upon the existing body of work by NIST on IoT security (referred to in this report in previous years).

This year's research for the report added 34 new device manufacturers. The report continues to track a widened dataset following the re-calibration in 2023's report. The dataset had a slight net increase in 2024 as 22 manufacturers were removed - 20 are no longer exist or have ceased selling IoT products and two were removed as duplicate entries (see Errata section). The original, core dataset of companies selected in the first report will no longer be reported on.

The headline statistic for this year's report is that 35.59% of global IoT manufacturers have a vulnerability disclosure policy, meaning that 64.41% have no way for security researchers to contact them. This marks a 11.60% increase in adoption of vulnerability disclosure best practices since the 2023 report against the expanded dataset which had at that point shown a slight dip in the original overall trend due to the expansion. It demonstrates that even the 'long-tail' of IoT manufacturers are starting to adopt better security practices.

As retailers in the UK particularly are now liable for their adherence to the PSTI Act's Regulations[2], additional research in this report has been conducted to focus on some of those retailers in order to further understand from which manufacturers the stocked products come from.

*1. https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf*

*2. https://www.gov.uk/guidance/regulations-consumer-connectable-product-security*

## What is vulnerability disclosure?

As outlined in the 2023 report and reiterated here, the concept of vulnerability disclosure grew out of the hacking community to eventually become standardised and adopted as good practice by many in the technology world, including governments. The European Union Agency for Cybersecurity (ENISA) defines vulnerability disclosure as "the process of identifying, reporting and patching weaknesses of software, hardware or services that can be exploited."[3]. Not only is this process important to avoid or rectify potentially critical issues in a product, but a clearly defined vulnerability disclosure scheme for a manufacturer can be an indicator of a positive general security posture[4].

The standardised best practice for vulnerability disclosure is called 'Coordinated Vulnerability Disclosure' or CVD. In this process the researcher contacts the company, the report is acknowledged by the company within a certain period (usually 24-48 hours) and then the company sets about investigating and addressing the vulnerability reported. Because all the reports are security related, it is likely that a swift resolution would be necessary – it is normally expected that reports are fixed in products within 30-90 days depending on the type of issue. If the security vulnerability requires a major hardware fix, it could be longer, but ordinarily the issue would be resolved with a software update pushed out to the products or services involved. At this point – the coordinated element takes place – the security researcher and the company would normally publish a notification and report of the discovered vulnerability. Often the security researcher would like to publish their results for a hacking conference or as an academic paper and this allows them to showcase their work and their efforts in discovering the reported vulnerability. In recent years, most hacking conferences require that CVD has taken place before a submitted talk is accepted. Overall, this process ensures that end users are not exposed to exploitation before a fix has been put in place by a company and it demonstrates that the hacking community are not interested in damaging businesses.

Implementing a vulnerability disclosure policy is easier than ever and there are free resources and tools to get an organisation started. Below is a table with resources to get an organisation started:

| Organisation | Resource | Link |
|---|---|---|
| UK NCSC | Vulnerability Disclosure Toolkit | https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf |
| Security.txt | Security.txt | https://securitytxt.org/ |
| IoTSF | Vulnerability Disclosure Best Practice Guidelines | https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf |
| | Consumer IoT Security Quick Guide: Manage Vulnerability Reports | https://iotsecurityfoundation.org/wp-content/uploads/2020/08/IoTSF-Vulnerability-QG_FINAL.pdf |
| Dutch NCSC | Coordinated Vulnerability Disclosure: the Guideline | https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline |

*IoT resources available online*

*3. https://www.enisa.europa.eu/topics/vulnerability-disclosure*

*4. https://www.ncsc.gov.uk/files/NCSC-Vulnerability-disclosure-Toolkit-v2.pdf*

## Regions retailing IoT products

The first time this research was conducted, the researchers generated a list of global, major consumer retailers to gather IoT device manufacturers from. As with 2023, the list was reviewed in order to maintain a representative sample. To do this, the team ensured that retailers across all the regions outlined below were included to allow for regional comparisons; as legislation is progressing around the world retailers will have some responsibility for selling compliant devices.

- EMEA – Europe, Middle East, and Africa
- NA – North America
- LATAM – Latin America
- APAC – Asia-Pacific

Turkey has been included in the EMEA region as it is geographically in Europe and Asia but is usually categorised as a part of the EMEA business region.

# Methodology

**This is the seventh year of this report and its research. In 2018, Copper Horse started examining the adoption of vulnerability disclosure among manufacturers of popular consumer IoT devices as a way to measure whether companies were adopting best practices on IoT security. Vulnerability disclosure policies are one of the few public indicators that give this information – they're either on a company's website or they're not. These are what are considered 'insecurity canaries'. With each year that passes and with each annual review of the data, companies are removed from the research dataset. The main reasons for this are because companies cease operation or stop selling connected products. This year the dataset lost twenty-two companies.**

The terms manufacturer and vendor are generally used interchangeably in this report and it should be noted that all the retailers captured in this report have an online sales platform.

The research continues using the same methodology as previously although the time window during which the research was extended slightly due to Copper Horse staff availability. When the research was initially conducted, a list of global retailers used to gather manufacturers was built. The research team captured the most popular IoT devices by reviewing listings on the retailers in this list and usually sorting by the "best seller" metric. The retailer list is split evenly across the EMEA, APAC, NA, and LATAM regions. This year one of the retailers had ceased trading via its website, although the manufacturers stocked by that retailer had already been captured in the list in previous reports. Using the global retailer list, the team has gathered a total of 458 consumer IoT manufacturers selling products globally. This includes 34 new additions for 2024, while 20 companies were removed as they have gone out of business or stopped selling consumer IoT products and two were removed. as duplicates from the dataset.

This year's report continues to expand the core dataset of manufacturers, which was re-calibrated in the 2023 report following a number of companies going out of business and the emergence of new ones in the market which were retailing smart, connected products. The report therefore from this year tracks only the expanded dataset.

## *Methodology (cont.)*

Interestingly, the headline figures for this year's report, based on a further expanded dataset, closely align with the predicted trend in 2023's report along the original core dataset. While last year's expansion saw a decrease in the percentage of companies with vulnerability disclosure policies, taking the overall figure to 23.99%, the original core dataset was trending higher and the predicted trend showed that it would likely be around 35% in 2024. The actual data shows the expanded dataset now aligns (at 35.59%) with that prediction, meaning that there has been a significant bounce of over 10% showing definite change in the market. In context however, it is still a relatively poor state of affairs – it is too early to state whether this is the beginning of the 'stick' part of the hockey-stick curve of adoption. Whatever the case, an increase in numbers of adoption is welcome.

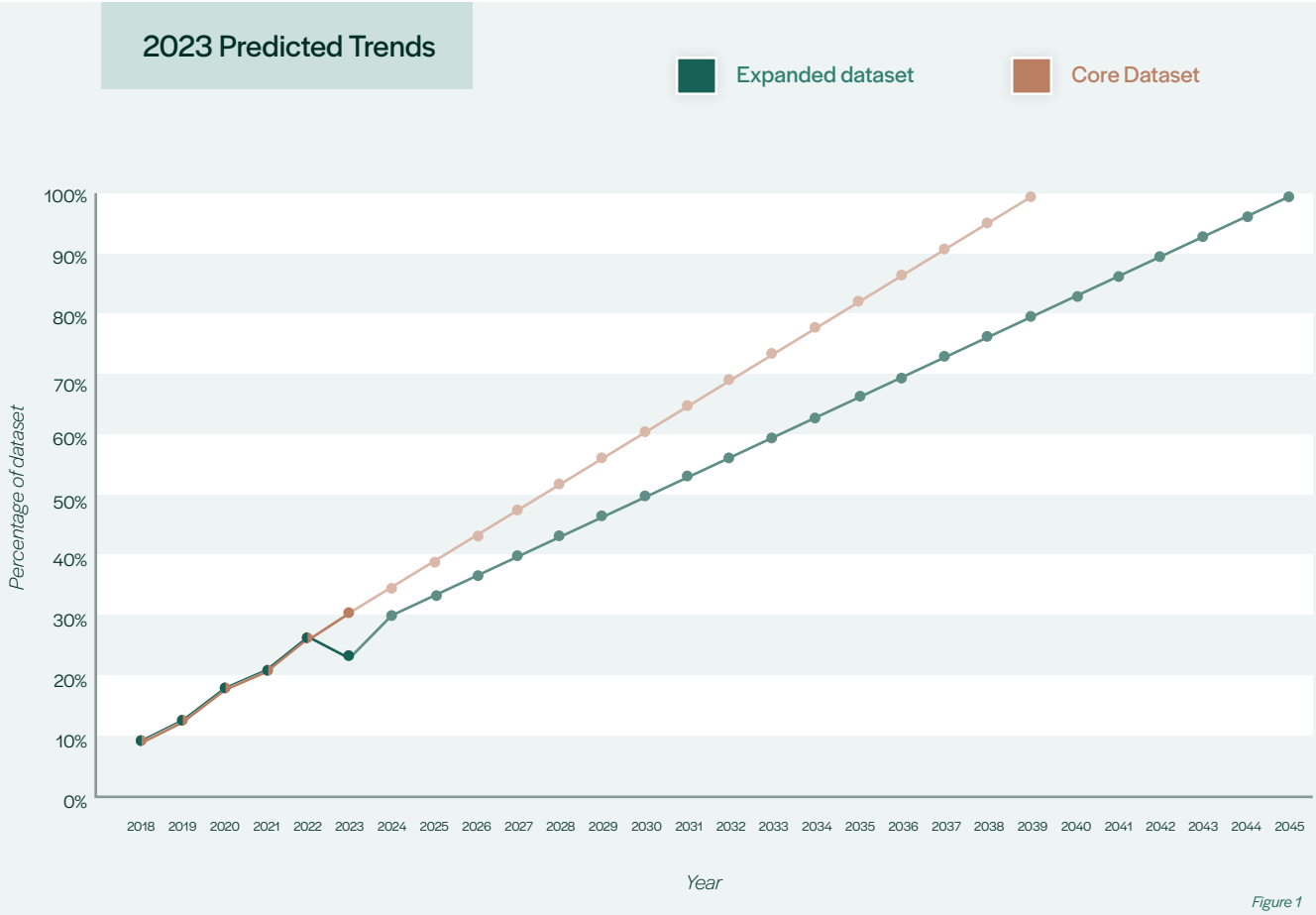



*Figure 1*

***2024's overall Dataset findings returns to the Core Dataset trend predicted in 2023***

Continuing last year's look at retailers, comparison analysis is provided on the products sold by retailers, which again seeks to understand to what extent retailers are stocking products from manufacturers that adopt good security best practice, in the form of vulnerability disclosure policies.

As with previous reports, the entire dataset is available as open data at copperhorse.co.uk

# Errata

## Dyson

In 2023 the report stated that Dyson did not have a vulnerability disclosure policy, however on further investigation it was discovered that the company had a vulnerability disclosure policy, a formal reporting system and an invite-only bug bounty program. Dyson has additionally offered an open-to-all bug bounty scheme which was launched in March 2024.

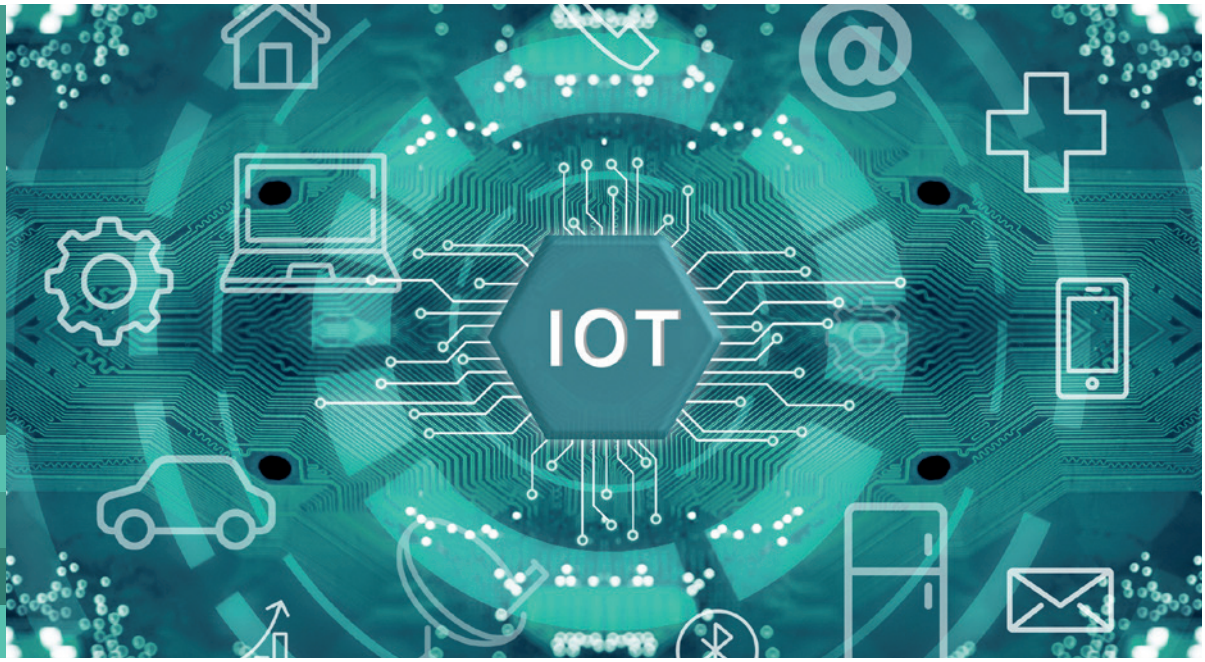
A re-published errata version of the report from 2023 has been published which explains this error, however the data was not adjusted. This should be taken into consideration if using the 2023 report.

## Duplicates

A review and data cleanup in 2024 discovered three duplicates in the list. Two of them listed out the same products for each entry. These were:

- Merkury Innovations (Smart Wi-Fi LED Bulb)
- Tado (Smart Thermostat)

The third duplicate may have come from Elgato being the parent company of Eve with the organisation selling products under two different names. The researchers listed one entry as Eve and the second as Elgato, Eve. These have both been retained and the second entry has been renamed to just Elgato.



# Key Findings

**This year's further widened dataset, based on last year's expansion, gives a more accurate picture of the state of the world's IoT product landscape, giving a better understanding of the application of product security by IoT manufacturers.**

## The Headline Figure

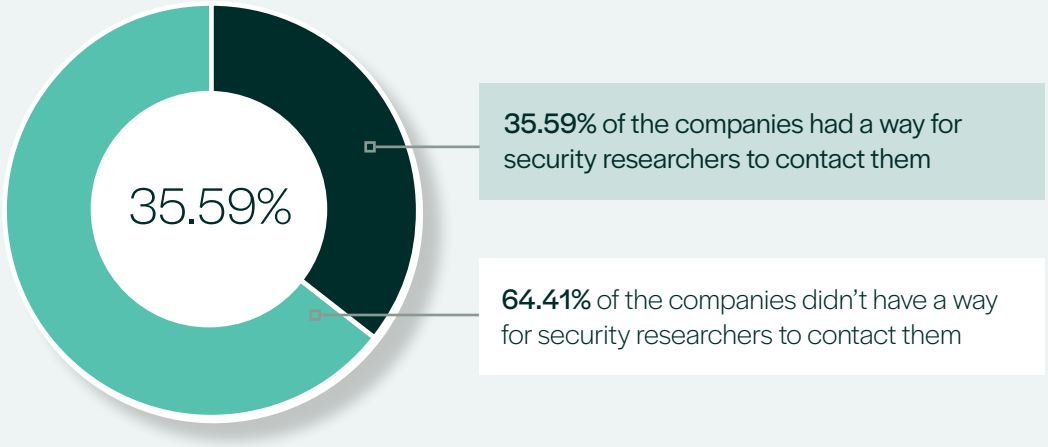
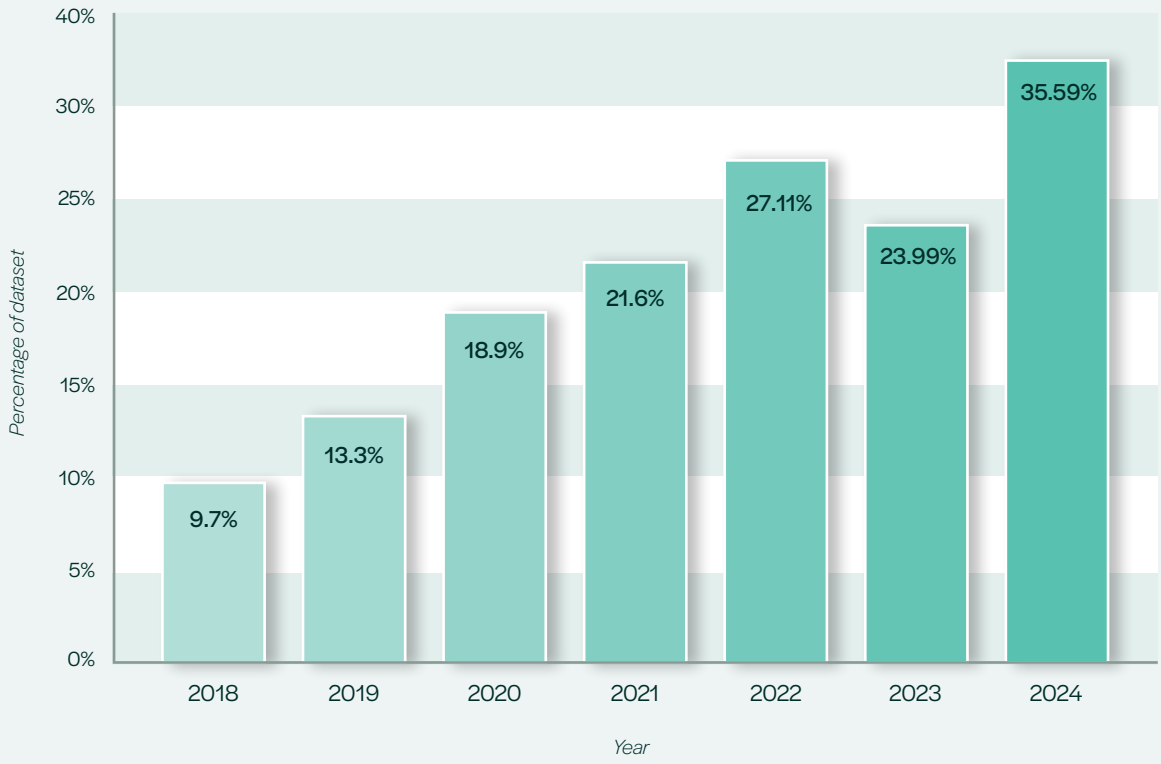



*Figure 2*

The 2023 report which had re-calibrated the landscape by extending the number of manufacturers covered resulted in a dip to the trend of vulnerability disclosure policy adoption (2022: 90/332 (27.11%), 2023: 107/446 (23.99%), over an expanded dataset. For 2024, with a slightly expanded dataset again, the figures are: 163/458 (35.59%) – a 11.60% increase in the total number of manufacturers in the dataset with a vulnerability disclosure policy. This means that 64.41% of IoT manufacturers do not have a way for security researchers to report security issues, a number that generally continues the original trend of adoption that has been seen in this report since its inception. Given the expanded scope and subsequent dip in adoption percentage in 2023's report, this appears to indicate the biggest yearly increase in adoption since the report started.

## Vulnerability Disclosure in Practice Trend

*Figure 3*




# Retailers

The research stage for this report is conducted annually and new manufacturers have been captured and added to almost every report, both to account for companies no longer operating or selling connected devices and to ensure the dataset remains representative of the current popular IoT manufacturers. The 2023 research data was the first time those new companies impacted the entire percentage so greatly. All of the retailers Copper Horse researched in 2024 to gather new manufacturers, saw similar levels when it came to stocking products from IoT manufacturers that supported vulnerability disclosure policies or not. In 2024, one of the retailers in South Korea, 11Street had ceased trading[5]. Where possible the researchers discovered other retailers which also stocked the products found at 11Street. The APAC region how has 3 retailers in the research set (down from 4), as does the LATAM region.

This report found that in 2023 UK and EU retailers had very similar levels of compliance at 23/41 (56.10%) and 38/67 (56.72%) respectively, with the US further behind at 22/58 (37.93%). The 2024 data demonstrates that all retailers have improved with UK retailer compliance at 55/75 (73.33%). The picture in the EU also saw an increased level of compliance among manufacturers of popular products on the platforms at 43/70 (61.43%). US retailers' compliance improved to 29/64 (45.31%) of manufacturers of the popular IoT products with a vulnerability disclosure policy.

*5. https://www.koreatimes.co.kr/www/biz/2024/10/602_366608.html*

# The threshold test

Each year since 2020, this report provides statistics of which companies pass a threshold test in relation to their implementation of vulnerability disclosure on their websites. The PSTI Act regulatory requirement for vulnerability disclosure is the basis of the threshold test.

The threshold test consists of two parts:

1. Have a vulnerability disclosure policy &;
2. Provide some kind of information on expected timelines

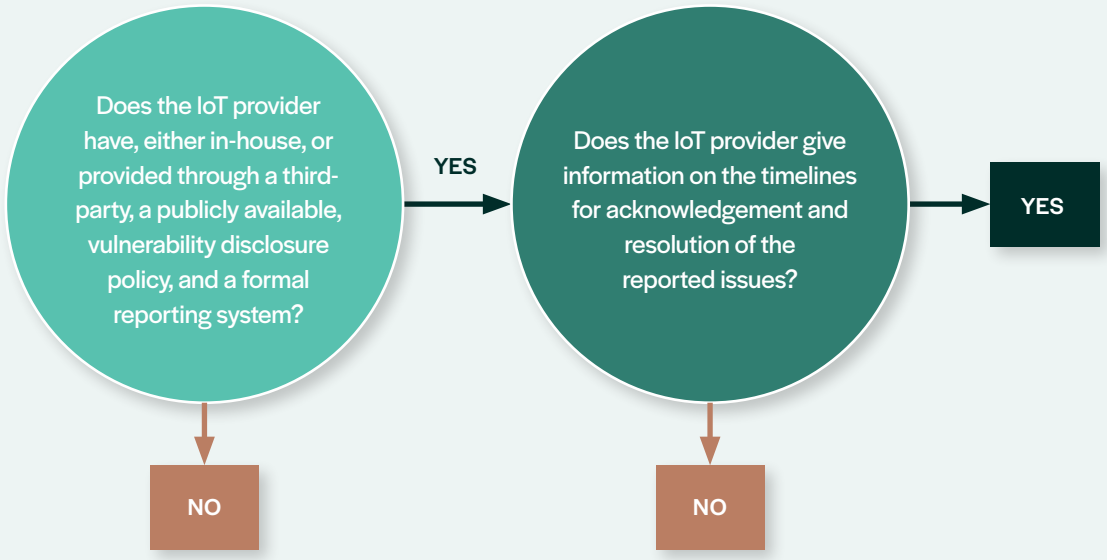
The researchers examined the data and found that the number of companies that pass both parts of the threshold test has increased significantly to 97/458 (21.18%) in 2024 – over double that of the previous year's 42 (42/446 - 9.42%). The number of companies that only pass the first part of the test has decreased in percentage terms from 65/446 (14.57%) in 2023 to 66/458 (14.41%). The remaining vendors represent 64.41% (295/458) of the dataset.

**The number of companies that pass both parts of the threshold test has increased significantly to 21.18% in 2024.**

Once again this year, compliance to regulatory requirements for these manufacturers seems a distant prospect given that this subject has been talked about as good practice for many years now.

## Threshold Test

*Figure 4*



# Examining retailer prospective compliance

As discussed in the 2023 report, it is not only manufacturers that are responsible for selling products that meet basic security requirements. Retailers of connected devices have some measure of responsibility for the products sold in their outlets. The UK's PSTI Act states that the security requirements it contains must be complied with by retailers of connected devices. In the 2023 report, the Copper Horse team examined retailer prospective compliance based on the existing popular connected products listed. It was decided that the three regions the researchers would investigate were the EU, UK and US because, as stated earlier, intended regulation in these areas was currently the most mature. In 2024, this remains the case, with the PSTI regulations now active in the market.

This subset of research was conducted following a similar methodology to the main dataset. The researchers captured the manufacturers of popular IoT devices, at the time of research, listed on retailers from the EU, UK, and US. The retailers below were selected as they offer a representative sample of major retailers within the three identified regions.

| Region / Country (Number of Retailers) | Retailers | Stocked Manufacturers Using Vulnerability Disclosure 2023 | Stocked Manufacturers Using Vulnerability Disclosure 2024 |
|---|---|---|---|
| European Union (5) | CDiscount, France | 5/12 (41.67%) | 6/12 (50.00%) |
| | El Corte Ingles, Spain | 12/17 (70.59%) | 12/17 (70.59%) |
| | EPrice, Italy | 5/10 (50%) | 6/11 (54.55%) |
| | Media Markt, Germany | 7/8 (87.5%) | 8/10 (80.00%) |
| | Otto, Germany | 9/20 (45%) | 11/20 (55.00%) |
| United Kingdom (3) | Amazon UK | 3/14 (21.43%) | 7/15 (46.67%) |
| | Currys | 11/17 (64.71%) | 10/15 (66.67%) |
| | John Lewis | 9/10 (90%) | 14/15 (93.33%) |
| United States of America (3) | Best Buy | 8/18 (44.44%) | 13/23 (56.52%) |
| | Target | 8/10 (80%) | 8/12 (66.67%) |
| | Walmart | 6/30 (20%) | 8/29 (27.59%) |

*Table showing retailers and the manufacturers they stock that use vulnerability disclosure comparing 2023 figures with 2024*

As can be seen in the table, there are variations in the data, with some retailers slightly improving their number of product manufacturers supporting vulnerability disclosure, but others dropping compared with the previous year. The range of products is relatively low and do not compare with the huge volume of products available on online market places such as Amazon.

# UK Retailer Analysis

As the PSTI Act regulations are now active in the UK, the researchers explored other retailers, including the UK's largest toy store chain to better understand the market situation. Argos, Smyths Toys and Tesco were added to the existing list above. Smyths stocked less manufacturers of connected products: just one baby monitor, a kid's smart watch and some gaming and lighting accessories.

The following table shows that of the dip test products, most of the manufacturers of those products had a vulnerability disclosure policy, with the exception of Amazon UK and Smyths where less than half of the products' manufacturers had policies. In 2024, the UK 'dip test' of products was limited to the same maximum number of devices at each retailer as it was recognised that some retailers such as Amazon stock a huge number of connected products which vary hugely in price and quality.

| Retailers | Stocked Manufacturers Using Vulnerability Disclosure 2024 |
|---|---|
| Amazon UK | 7/15 (46.67%) |
| Argos | 13/15 (86.67%) |
| Currys | 10/15 (66.67%) |
| John Lewis | 14/15 (93.33%) |
| Smyths | 2/5 (40.00%) |
| Tesco | 9/10 (90.00%) |
| Overall | 55/75 (73.33%) |

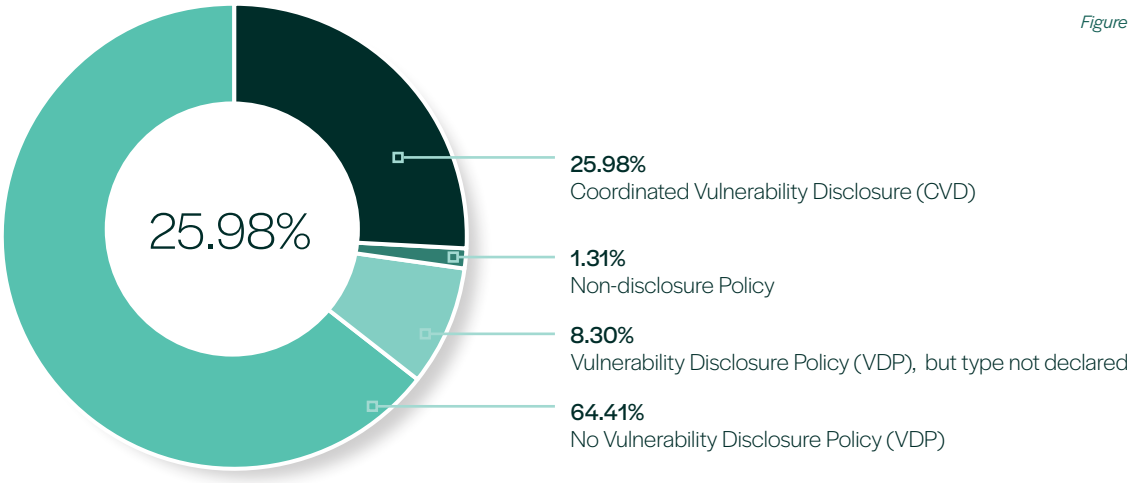
The UK slightly differs from the other regions, with some of the major retailers close to 90% in terms of the manufacturers stocked that support vulnerability disclosure policies. This is generally positive.

# Types of Vulnerability Disclosure

Coordinated Vulnerability Disclosure (CVD) is the industry recognised and internationally standardised, best practice for vulnerability disclosure. The security researcher and vendor work together to identify, rectify and issue a patch; then finally the vulnerability can be disclosed to the public by the security researcher. Data from previous years showed a majority of organisations that have a vulnerability disclosure policy use CVD as the preferred method. The story continues into 2024, with 119/163 (73.00%), showing growth compared with 70/107 (65.42%) in 2023. Of the companies with a policy indicating they have CVD - 163/458 (25.98%) of the entire dataset compared with 70/446 (15.70%) in 2023. This report notes a rise of 10.28% in the use of CVD against last year's overall total. Similar to 2023, a small number 6/119 (5.04%) of companies with a policy or 6/458 (1.31%) of the overall number of companies, have a "non-disclosure" policy.

**This report notes a rise of 10.28% in the use of CVD against last year's overall total.**

*Figure 5*




## Regional differences

Most of the manufacturers in the report's dataset are headquartered in either North America, Europe, or Asia. None of the relatively small number of vendors based in Oceania and Africa have adopted vulnerability disclosure policies, but for the first time a manufacturer based in South America, Intelbras has a limited scope policy covering some of their IoT products[6].

Once again, the number of vendors in Europe, North America, and Asia adopting vulnerability disclosure has increased on the 2022 and 2023 figures. Europe has increased by around 21% from 19/101 (18.81%) in 2023 to 47/118 (39.83%) in 2024, North America has changed from 50/172 (29.07%) to 65/173 (37.57%), and Asia from 38/153 (24.84%) to 50/147 (34.01%) with the current research.

### Manufacturer adoption of vulnerability disclosure across the world

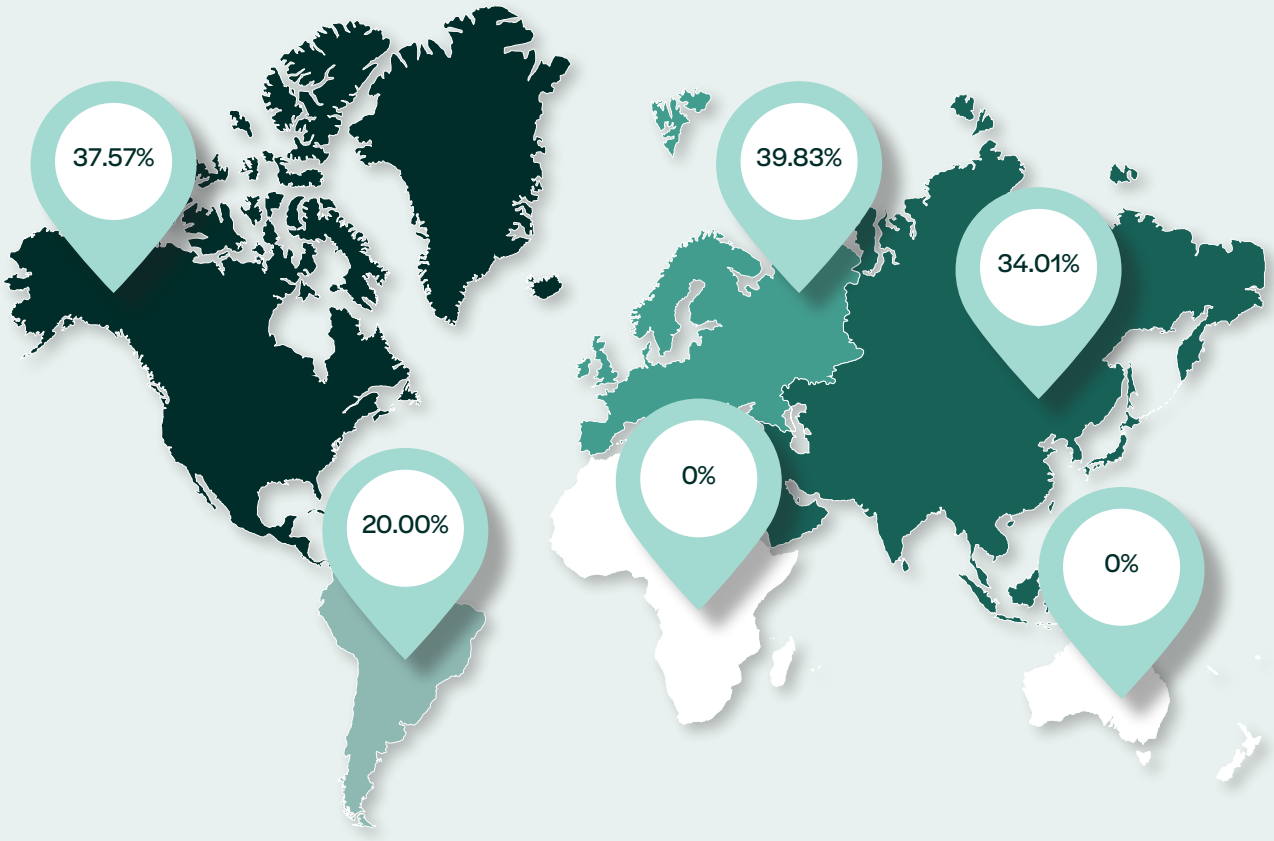



*Figure 6*

*6. https://www.intelbras.com/en/coordinated-vulnerability-disclosure-policy-intelbras*

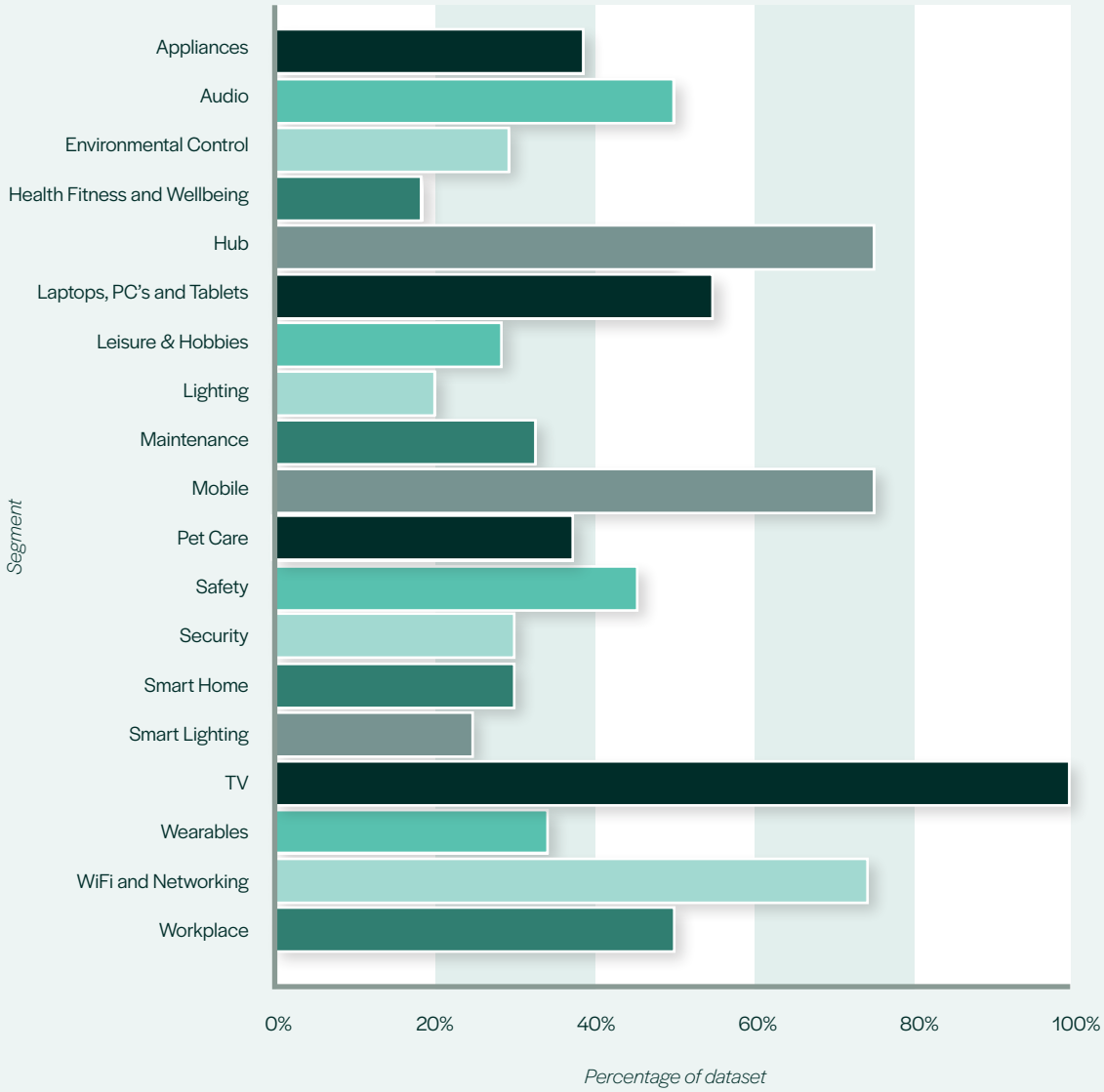
# Product categories

Product categories are the main type of product a consumer IoT manufacturer produces, targeted at a particular domain. It allows a breakdown of the data of how different manufacturers of connected consumer devices perform within the category of the type of device they offer. More mature product categories like TVs, Wi-Fi and Networking and Mobile consistently outperform less well-established categories such as Wearables. This year's research has shown that a number of product categories have seen quite significant percentage increases in adoption of vulnerability disclosure (taking into account that each category still has low individual numbers). The Audio, Appliance Environmental Controls, Leisure and Hobbies, Pet Care, Maintenance Wearables, Workplace product categories all saw significant increases over the 2023 data, with only the Wi-Fi and Networking category seeing a decrease.

Below are all the product categories captured in this research and the percentage of the category employing vulnerability disclosure.

## Percentage of Companies in a Segment with a Policy

*Figure 7*



## Enterprise

In 2021, the researchers examined a small group of enterprise or business-to-business (B2B) manufacturers. This dataset continually outperforms the other data in the report. The research carried out in 2023 found that 42/48 (87.5%) of those organisations had vulnerability disclosure policies, well over triple the core dataset value in that report. In 2024, the enterprise dataset remains the same and continues to be reviewed as the findings are still relevant. This year's data shows that 44/48 (91.67%) of the enterprise organisations had a way for security researchers to contact them, representing a 4.17% change This is a further positive sign for enterprise IoT.

## Proxy Disclosure & Bug Bounties

Organisations which do not have the capacity to operate a vulnerability disclosure programme or simply want to outsource it can do so by utilising proxy disclosure organisations, which will host the company's desired policy on the proxy platform. The research has found that 34/458 (7.42%) of manufacturers use a proxy disclosure organisation for vulnerability disclosure, a small increase on 2023's figures of 27/446 (6.05%). 2023's report saw the addition of BugBase, Intigriti and Yes We Hack as proxy disclosure organisations, to add to BugCrowd and HackerOne. The share of the IoT market using this method for disclosure is still very small as the comparison table below shows and BugBase has dropped out of the data.

| Category | 2023 | 2024 |
|---|---|---|
| Proxy Disclosure Organisations | N/A 419/446 (93.95%) | N/A 423/458 (92.36%) |
| | HackerOne 13/446 (2.91%) | BugCrowd 16/458 (3.49%) |
| | BugCrowd 11/446 (2.47%) | HackerOne 16/458 (3.49%) |
| | BugBase 1/446 (0.22%) | Intigri 1/458 (0.22%) |
| | Intigri 1/446 (0.22%) | Yes We Hack 2/458 (0.44%) |
| | Yes We Hack 1/446 (0.22%) | |

Some manufacturers choose to offer bug bounties alongside a vulnerability disclosure scheme. A bug bounty is simply a mechanism for offering a financial reward to encourage security researchers to submit vulnerabilities to a manufacturer, as a way of incentivising and rewarding participation. These bug bounty schemes typically include a scope which outlines the products and services a manufacturer makes available to test, and the financial reward a researcher can receive for each category of bug. The research in 2024 observed that 38/458 (8.30%) of manufacturers in the dataset used this method for engaging with researchers, the figure captured in 2023 was 29/446 (6.50%), a nearly 2% increase on the previous year, but still a low number relative to the overall dataset.

## Use of /security pages & Use of security.txt

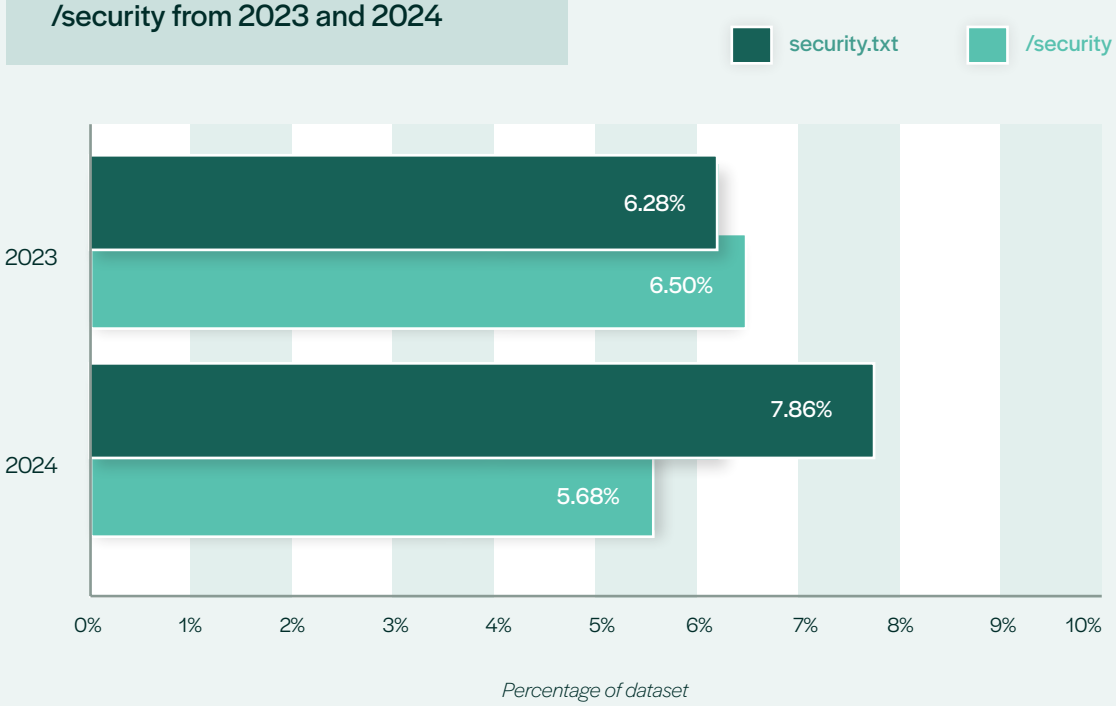
The research conducted in 2023 found for the first time, that the number of organisations using security.txt files (located at /.well-known/security.txt) was higher than the number of organisations placing its vulnerability disclosure policy on a /security page and this trend has continued into 2024, with the gap slightly widening and the numbers of manufacturers with a /security page decreasing by two, against a wider dataset – (in 2024 26/458 (5.68%) versus 2023's 28/446 (6.28%).

There has only been a small rise in the use of security.txt of 1.36% since the last report (2023: 29/446 (6.50%) and 2024: 36/458 (7.86%). Once again, the relative overall change to this data is however fairly static.

As observed in 2023, /security web pages have been captured as a location for storing a vulnerability disclosure policy throughout these reports, being recommended in the IoTSF's publication Vulnerability Disclosure Best Practice Guidelines[7]. However, they aren't as universally applicable or specifically usage-reserved as a security.txt file would be. The location '/security' on a manufacturer's site may already be used for other purposes - to hold information about security related products, for example, security.txt offers a standardised location, as well as a defined format for information about a vulnerability disclosure policy. There is much progress to be made in this area and in vulnerability disclosure more broadly and it may be that guidance on vulnerability disclosure by recommendations and standards bodies should by reviewed in order to take into account the standardised location of security.txt. The security.txt standard is a universally applicable location, however the number of companies adopting it remains very low.

Comparing usage of security.txt and /security from 2023 and 2024

*Figure 8*




*7. https://iotsecurityfoundation.org/wp-content/uploads/2021/09/IoTSF-Vulnerability-Disclosure-Best-Practice-Guidelines-Release-2.0.pdf*

## PGP keys

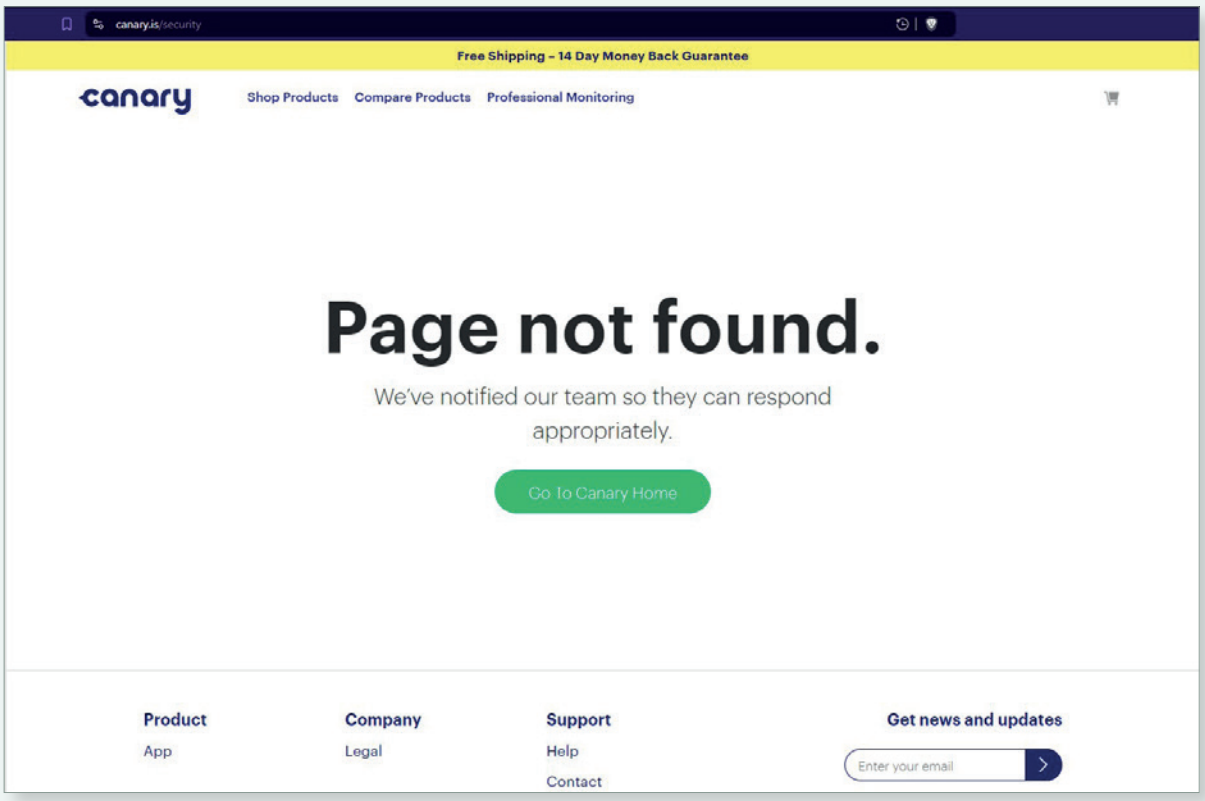
In 2022, this report captured an approximately 14% decrease in the usage of PGP keys to encrypt vulnerability reports, with 52/332 (15.66%) of the manufacturers offering it in 2022. 2023 saw 57/446 (12.78%) using PGP. While the manufacturer numbers slightly increased, the percentage decreased again with the larger dataset. In 2024, the percentage trend has returned more closely to the 2022 figures, with 65/458 (14.19%) of manufacturers providing PGP keys for researchers to use when contacting them.

# Talking Points and Observations

This section includes some observations and talking points derived from things that have been seen when researching the companies in the report.

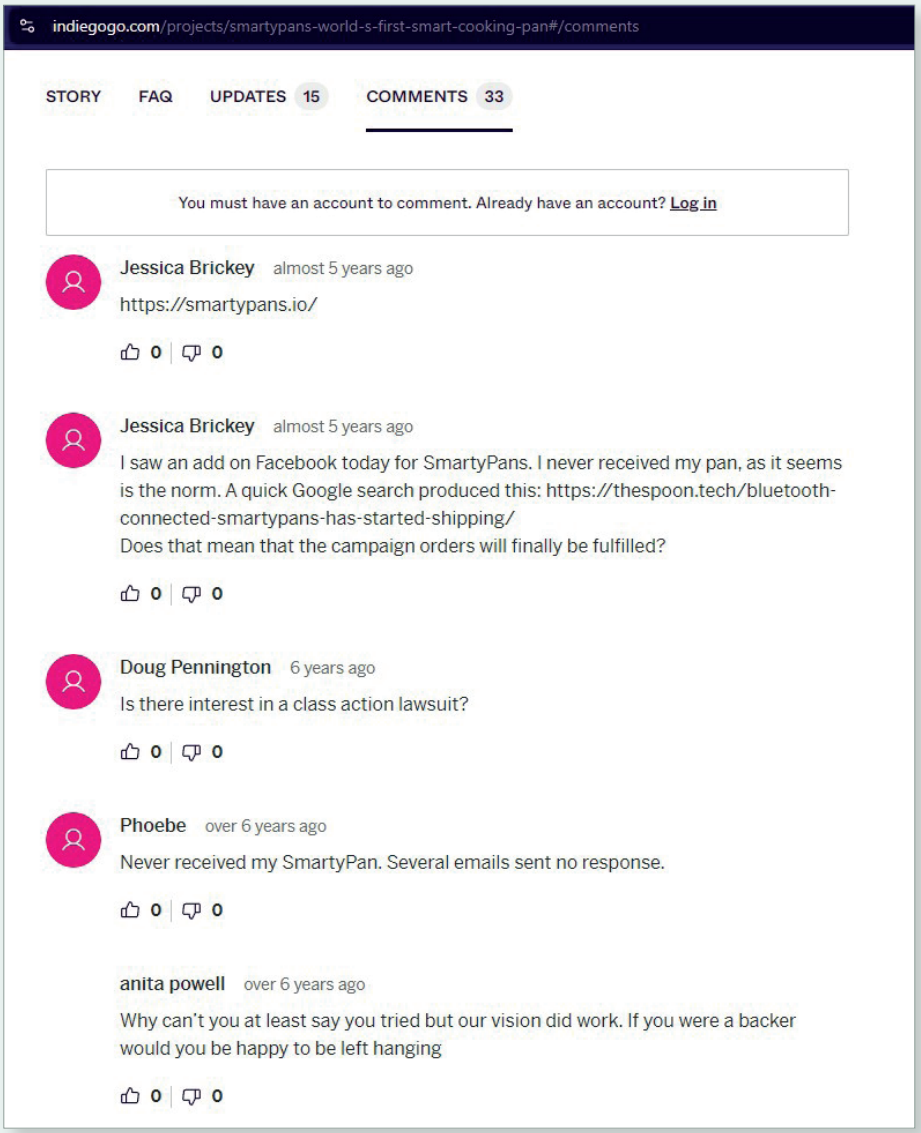
## Canary.is

In 2023 the company had a vulnerability disclosure policy however this no longer exists. The company's contact address doesn't exist at all on the site after extensive searching to check this.



## SmartyPans

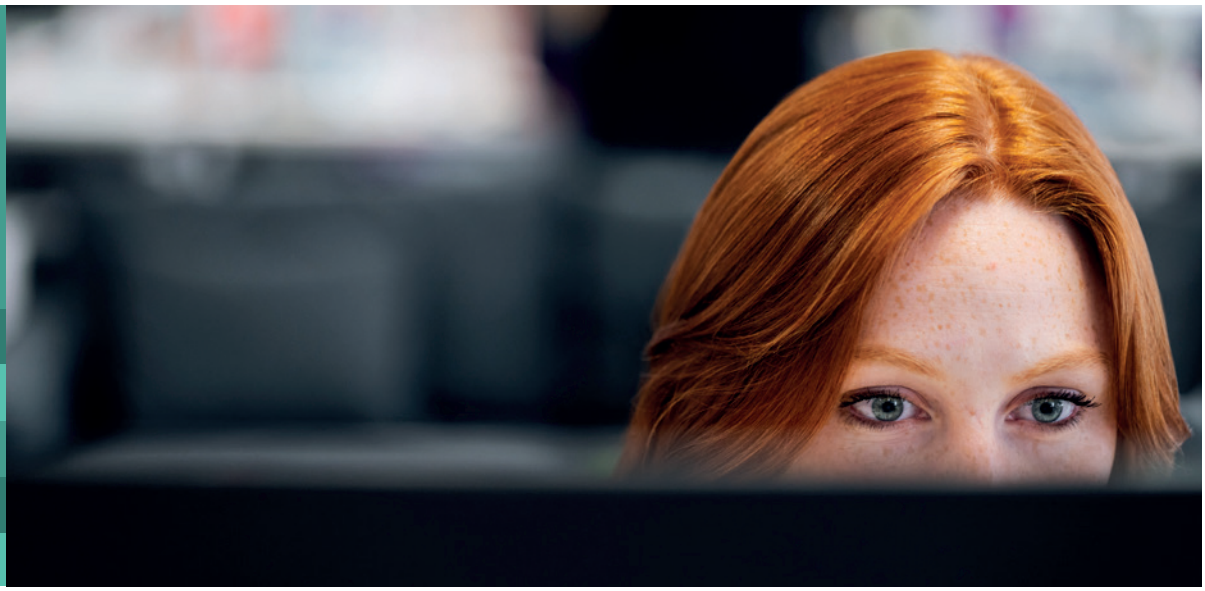
This was a site selling connected pans when Copper Horse's researchers checked it in 2023. The site has reverted to a waiting list. The website is still functioning and it is possible the company is launching a new product. The original indiegogo launch for the product was around six years prior to this report. Many of the comments suggested customers never received what they paid for:
https://www.indiegogo.com/projects/smartypans-world-s-first-smart-cooking-pan#/comments



## Mentions of PSTI

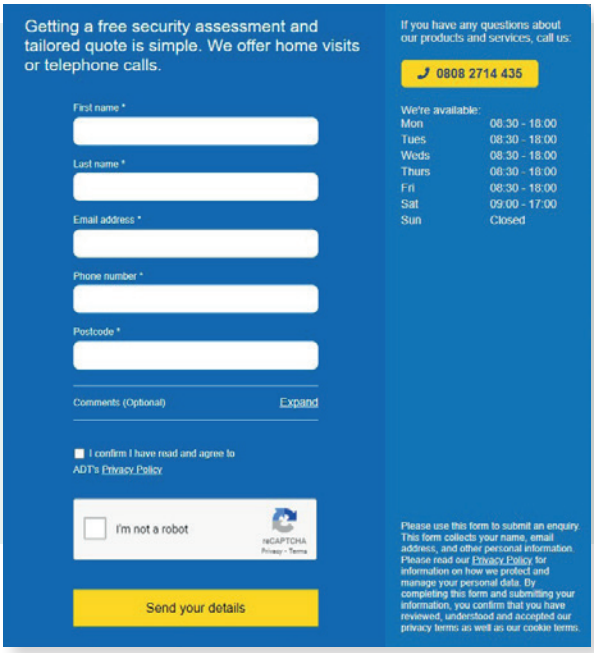
A number of companies were observed to be aware of the UK's PSTI Act. The following was observed:

- TPLink statement of compliance: https://www.tp-link.com/uk/psti/
- Logitech UK PSTI ACT 2022 Information: https://www.logitech.com/en-gb/legal/uk-psti-act-2022.html
- Yale Home PSTI Statement of Compliance: https://yalehome.co.uk/
- Linksys PSTI statement of compliance: https://downloads.linksys.com/support/assets/others/UK_PTSI_Statement_of_Compliance_w_products.pdf
- Hoover: "Due to the Product Security and Telecommunications Infrastructure (PSTI) legislation. New enrolment onto the wizard app will be blocked from April 29th 2024.": https://service.hoover.co.uk/advice-centre/hoover-wizard-wi-fi-help/
- Audio Pro PSTI Act 2022 compliance: https://uk.audiopro.com/pages/ptsi-act
- Roberts Radio PSTI Statement of Compliance: https://www.robertsradio.com/en-gb/PSTI
- Drayton Controls (part of Schneider Electric) UK PSTI Statement of Compliance: https://www.draytoncontrols.co.uk/sites/default/files/2024-07/BRU138720002-00%20Artwork%20Wiser.pdf
- Blueair: The UK Product Security and Telecommunications Infrastructure (Product Security) regime-Statement of Compliance: https://www.blueair.com/on/demandware.static/-/Library-Sites-blueair-eu-content-library/default/dw808f75e0/Compliance/UK_Letter%20of%20Compliance_Signed%202024-05-28.pdf
- energenie4u: https://energenie4u.co.uk/support/psti-declaration, not to be confused with their own PSTI (Privacy, Security, and Transparency Initiative (PSTI) Policy): https://energenie4u.co.uk/res/pdfs/privacy_security_and_transparency_initiative_(psti)_policy.pdf
- Casio PSTI Report a Vulnerability: https://www.casio.co.uk/psti
  (see notes below about the issues with this reporting mechanism)



## *Mentions of PSTI (cont.)*

- Blog on ADT site mentions PSTI:
  https://www.adt.co.uk/blog/are-diy-security-systems-vulnerable-to-hackers
  The blog states: "Manufacturers must provide a public point of contact so anyone can report a vulnerability." – however, when the report researchers searched for a vulnerability disclosure policy one could not be found. The only way to contact ADT was either through the app (if an ADT user) or through the companies web-portal:




ADT's parent company Johnson Controls does have a policy, however it's not linked directly on the ADT page and only on the Johnson Controls website:
https://www.johnsoncontrols.com/trust-center/cybersecurity/response

- Twinkly has a test certificate supplied by Intertek outlining a certification to the UK's PSTI Act regulatory requirements: https://help.twinkly.com/hc/en-gb/articles/18277836561053-PSTI-Certification


intertek

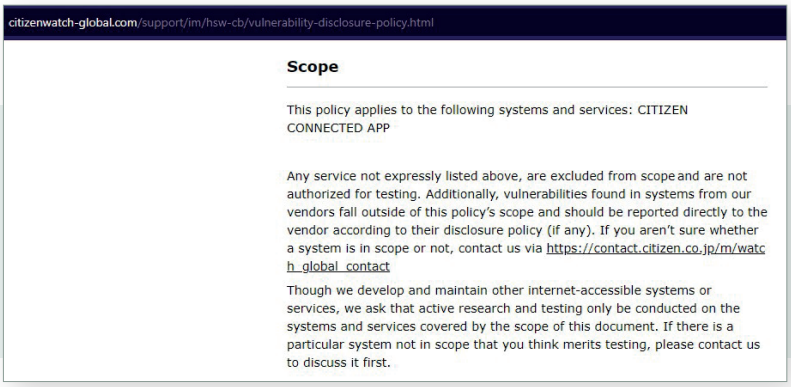
Test Verification – PSTI

Verification Number: 240318039SZN-VOC001

*Twinkly PSTI Test Verification Certificate, source:*
*https://help.twinkly.com/hc/article_attachments/19539588058269*

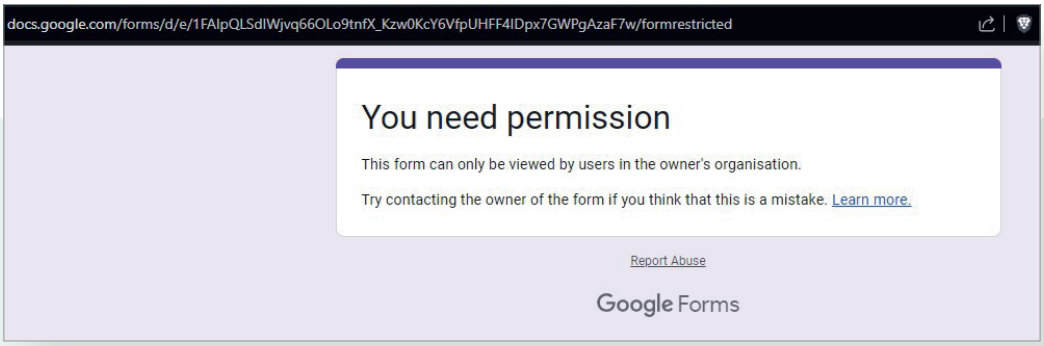
## *Mentions of PSTI (cont.)*

- Sekonda website confirming adherence to the PSTI Act provisions and to ISO/IEC 29147 (vulnerability disclosure): https://www.sekonda.com/smart-psti-act
- Skylight PSTI Statement of Compliance website: https://www.skylightframe.com/psti-compliance/
- Citizen Smart Watch P991 Vulnerability Disclosure Policy (VDP) and PSTI Statement of Compliance. This is interesting because the VDP is limited to the 'CITIZEN CONNECTED APP' (not the products themselves or anything else related). This may imply that Citizen don't produce this watch themselves, it is just a white-label product that Citizen have put the company brand on. Whatever the case, this is unusual and would seem to make them non-compliant with the PSTI Act: https://www.citizenwatch.co.uk/smart-psti-act




*Citizen Vulnerability Disclosure Policy, limiting disclosures to the CITIZEN CONNECTED APP – anything else is 'not authorized for testing'. Source: https://www.citizenwatch-global.com/support/im/hsw-cb/vulnerability-disclosure-policy.html*

- Casio's website has a 'PSTI Report a Vulnerability' page. In the 2023 report, they had no way for security researchers to contact them, so this is a direct example of the PSTI Act changing things for the better. This, however is incorrectly implemented. The vulnerability policy gives the company a green status on the threshold test, however the disclosure webform is inaccessible, because the permissions have been set incorrectly: https://www.casio.co.uk/psti




*Web form on the Casio PSTI vulnerability disclosure web page, which is inaccessible: https://docs.google.com/forms/d/e/1FAIpQLSdIWjvq66OLo9tnfX_Kzw0KcY6VfpUHFF4IDpx7GWPgAzaF7w/formrestricted*

*Mentions of PSTI (cont.)*

## Use of out-of-date vulnerability scoring

- boAT (a manufacturer of various connected products including ear buds and smart watches), is still using the CVSS2 vulnerability scoring system on their website boAT Lifestyle. The scoring system is no longer in use and was deprecated in 2022[8]: https://www.boat-lifestyle.com/pages/security. The company's website states that "CVSSv2 will be used as a reference standard for assessing and prioritizing vulnerability/vulnerabilities". In addition, boAT was hacked in 2024, with 7.5 million customer details leaked. https://www.business-standard.com/companies/news/data-of-7-5-mn-boat-customers-leaked-on-dark-web-forbes-india-report-124040800627_1.html
  The company has ceased using BugBase for proxy disclosure.

## Baby monitors

In 2024 the researchers of this report observed a significant number of suppliers offering baby monitors which have a camera and self-contained video screens, rather than connecting the baby monitor to the internet and potentially exposing vulnerabilities to hackers, as happened with Foscam in 2013[9].

*8. https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator#:~:text=The%20scores%20are%20computed%20in,Existing%20CVSS%20v2.*

*As of July 13th, 2022, the NVD no longer generates new information for CVSS v2.0. Existing CVSS v2.0 information will remain in the database but the NVD will no longer actively populate CVSS v2.0 for new CVEs. This change comes as CISA policies that rely on NVD data fully transition away from CVSS v2.0. NVD analysts will continue to use the reference information provided with the CVE and any publicly available information at the time of analysis to associate Reference Tags, CVSS v3.1, CWE, and CPE Applicability statements.*

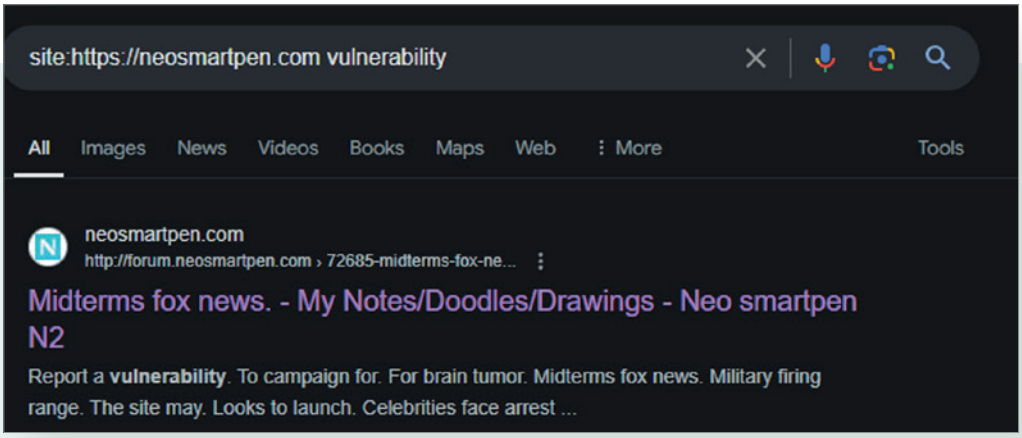
*9. https://www.bbc.co.uk/news/technology-23693460*

## Several suppliers have disappeared

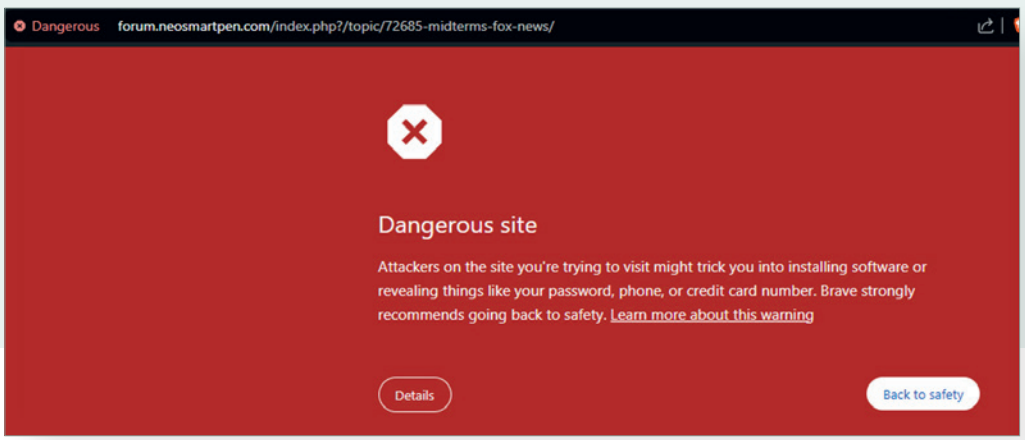
As the research has been conducted for a number of years now, a number of companies have gone out of business and/or their websites have disappeared. In 2024, 20 manufacturers have gone out of business or ceased selling appropriate products. One retailer is no longer in business with several of the generic smart watches no longer being available: http://global.11st.co.kr/. Manufacturers that no longer exist are removed from the research data for that year's report.

## Broken links

Searching https://neosmartpen.com for vulnerability reporting gave a strange forum link and then a warning that appeared to show that the website had been hacked and was hosting malware:




On clicking the link:



# Conclusions

**2024's report continued to expand the IoT manufacturer dataset as new companies are stocked within retailers. From the original 332 manufacturers, the report now covers a total of 458. All of the data is available to download under a Creative Commons 4.0 license for transparency and for further study by other researchers interested in this topic.**

The Copper Horse researchers who worked on this year's report expected to see a more pronounced upwards trend with regulation now active in the UK and further progressing in the USA and Europe. It is possible that this has happened, but it will not be obvious until 2025 whether this is the desired bottom of the hockey stick and the start of a huge trend upwards. In 2023, the expansion of the dataset resulted in what seemed like a correction to the statistics – a downward spike which may have possibly been associated with an expansion to the 'long tail' of the IoT market and therefore perhaps products of lower quality. The current year's data has seen a return to the original trend line as the original dataset, which was originally heading towards 2049 as the year when the market 'might' reach 100% adoption of vulnerability disclosure methods by manufacturers. One positive was the number of companies that pass both parts of the threshold test and which met the 'green' category demonstrating that they would comply with regulations, doubling that of the previous year; but still only representing around 20% of the overall market. The enterprise IoT data showed a further increase in adoption of disclosure policies, taking it to over 91% of the manufacturers surveyed, a very positive indication.

There has clearly been some effect from the UK's Product Security and Telecommunications Infrastructure Act (Part 1) requirements as the Talking Points and Observations section in this report

## *Conclusions (cont.)*

shows, but implementation seems fragmented and inconsistent. While some leading UK retailers are showing that around 90% of the IoT manufacturers they stock have vulnerability disclosure policies, there are some notable exceptions to this 'dip test' of the market and there are obvious differences in online marketplaces. The other regions showed less promising and variable data about the product manufacturers they stocked.

Readers of the report may see the overall market situation as inadequate. These manufacturers have all known for a long time that governments across the world have been seeking to bring in stricter measures, including the adoption of vulnerability disclosure, yet hundreds of companies in this dataset have done nothing. It is industry best practice and has been standardised for years so there should be no real excuse for not adopting it, yet it appears there are real barriers to adoption. It is for governments to decide what they do about this, particularly in the UK where it is a legal requirement. Companies in Europe will have until 2027 to achieve compliance to the CRA.

This report remains the most comprehensive, long-running and expansive study into vulnerability disclosure in the consumer and enterprise IoT space. The data will remain open and available for others to study and use.

# Annex

## This annex represents the output of the threshold test.

- **Companies highlighted in green pass both test 1 & 2 of the threshold test:**
  Has a vulnerability disclosure policy and provides information on expected timelines
- **Companies highlighted in amber pass only the first part of the test:**
  Has a vulnerability disclosure policy but no timeline information
- **Companies highlighted in red do not pass either part of the test, meaning:**
  Has no vulnerability disclosure policy or timeline information

| | | |
|---|---|---|
| Airthings | Hoover | Qnap |
| Anker, Eufy | HP | Reflex Active |
| Arris (Commscope) | HTC | RENPHO |
| Best Buy, Insignia | Huawei | Reolink Digital Technology |
| BlueAir | June | Ring |
| Bosch | IglooHome | Roberts Radio |
| BroadLink | Intelbras | Roku |
| Brother Industries, Ltd | iRobot | Samsung (SmartThings) |
| BT | Lenovo | Schlage, Allegion |
| Café | LG | Segway |
| Candy | Logitech | Seiko Epson |
| Casio | Logitech, Ultimate Ears | Sengled |
| Citizen | Lorex | Shark |
| Dell | Meross | SonicWall |
| Drayton | Meta | Sonoff |
| Dyson | Microsoft | Sonos |
| Ecobee | Midea | SUUNTO |
| Eero | Miele | SWANN |
| EGLO | MOTOROLA | SwitchBot |
| Elgato, eve | Motorola Mobility | Synology |
| EZVIZ | NanoLeaf | TP-Link |
| FIBARO | Neff | TVT |
| FireAngel | Netatmo | Twinkly |
| Foscam | Nuki | Voxx International, Klipsch |
| Fossil | Omron | Western Digital |
| Frameo | OnePlus | Whisker |
| Furbo | ONKYO | Wink |
| Gardena | OPPO | Withings |
| Google | Panasonic | WyzeCam |
| Hangzhou XiongMai Technology | Peloton | Xiaomi (MI) |
| Hanwha, Wisenet | Pico | Yamaha Pro Audio |
| HMD Global (Nokia Mobile) | Procter & Gamble, Oral-B | Yamaha Corporation |
| HONOR | Qardio | |

## *Annex (cont.)*

| | | |
|---|---|---|
| Acer | FLiR | Samsung (Galaxy Watch) |
| Amazon | Garmin | Samsung (Mobile) |
| August | GE Appliances | Samsung (Smart TV) |
| Apple | Hikvision | Sekonda |
| ARLO | Hive | Siemens |
| ASUS | Honeywell Home (Resideo) | Signify - Philips Lighting |
| Audio Pro | JBL | SimpliSafe |
| AVM | Lexmark | Skylight |
| Belkin | Lifx | Sony |
| Beurer | Linksys | Sphero |
| BLINK | Lovense | Tapplock |
| boAt | Loxone | Tefal |
| Bose | Marshall | TomTom |
| Buffalo | Nespresso | Trane |
| Canon | Netgear | Tuya |
| Dahua | Oura | Vivo |
| Devolo | PetCube | Vtech |
| D-Link | Philips | WiZ (Signify) |
| Draytek | Phyn | Yale |
| Energenie | Rachio | Yummly |
| Eve | Ray-Ban | ZTE |
| FitBit | Ruark | ZyXEL |

| | | |
|---|---|---|
| 360 | ANTELA | Baytion |
| 116 Plus | ApnaCam | BeBird |
| 2NLF | Apollo Tech USA | Beeline |
| ACEMAX | Apption Labs | Behmor |
| ACTi | Aqara | BELLABEAT |
| AdhereTech | Aranet | Blackview |
| ADT | ARKIFI | BLU Products |
| Aeon Labs, Aeotec | Armani | Calex |
| Airboxlab | (Armani Exchange, Emporio Armani) | Canary |
| Aiwa | Arugo | Canon, IRIS |
| AKILII | ASAKUKI | Catapult Sports |
| AliveCor | Ation | Chamberlain |
| Amaryllo | Atom Labs | Chamberlain |
| Amazfit (Huami) | Aubess | Circle |
| Amor Gummiwaren GmbH | Aura | Clever Dog |
| Amped Wireless | Avidsen | Click and Grow |
| Anmossi | Awair | COA |
| Anoto | B&O | Comap |
| Anova | Bangtan | CP Plus |

## *Annex (cont.)*

| | | |
|---|---|---|
| Cresta | Greater Goods | Klarstein |
| CTRZQ | Grohe | Kobo |
| Cube | Groove | Kolibree, Baracoda |
| Curb (Powered By Elevation) | Guardian Technologies (Lasko) | Konnek Stein |
| Current Labs | Hama | Koogeek |
| Daybetter | Hank | Kwikset |
| DCU | Hatch | Lampaous, LUMENMAX |
| Deeper | Hatch Baby | Laresar |
| Delta Five | HAVIT | Laurastar |
| DENON | Haylou | Lenbrook Industries, Bluesound |
| Devialet | HeimVision | Leotec |
| DEWENWILS | Hidrate | LetsFit |
| DigitalKeys | Hoco | LifeFitness |
| Diyarts | Hombli | LIGE |
| Doogee | HTN | Lightwave |
| Double Robotics | Hunterfan | Lithe |
| Echel | Husqvarna | Lockstate, smartLOCK, RemoteLOCK |
| Edimax | Hyiear | Lohas |
| Einhell | Hyrican | Luckwolf |
| ELAiCE | iFanze | lulshou |
| Elecom | iFAVINE | Lutron |
| Eminent | IFITech | Matrix |
| EMOOR | iHealth | Mattel, Fisher-Price |
| Enabot | iHuniu | Maxevis |
| eq-3 | iku | MEGABRIGHT |
| Estimote | ilumi | Merkury Innovations |
| Etekcity | InBody | Michael Kors |
| F22 | Infinix | MIPOW |
| Feit Electric | INLINE | Moen |
| First alert | Innr | Moes House |
| FITPRO | Insteon | MoKo |
| Flux Smart | InteraXon Inc | Moleskine |
| FREDI | iReader | MSI |
| Garadget | Iris Ohyama | Muvit |
| GARETT | Jasco | MySpool |
| Garza | Jura | NAIM |
| Gavdhe | JUSTGREENBOX | Nautica |
| Geekee | Kangaroo | Neato |
| Genius Hub | Keen Home | Neo |
| GNCC | KeySmart | Neurio, Generac |
| Goldair | Kickstart | Neutron |
| Gosund | Kidde | NEXXT SOLUTIONS |
| Govee | KIQULOV | NGTeco |

## *Annex (cont.)*

Night Owl
Nivian
Noise
NordicTrack
Novostella, Ustellar
Osram
Otio
Overmax
Oyajia
Perfect Company
PetLibro
Pixbee
Plus Style (+Style)
PNI
Polar
Popglory
Positivo
Proform (ICON fitness)
Promate
Qrio
RADEMACHER
Radley
Ratoc Systems
Razuvious
Remotec
Roost
Ruveno
Sacramento
Seneye
Sensibo
Sensoria
Shenzhen Neo
Simpled
SIXPAD (MTG)
SKY HUB
Skybell
Sleep Number
Small
Smartbell
Smarter Applications
SmartPlate
SmartyPans
SMD Technologies branded as Connex Connect
SNARIYOVSN
SOSAFE
SpaceTalk
SSC-LUXon
Steren
SWAN
Tado
Tanita
TCL Corporation (Alcatel)
Teckin
Teckin
TEKXDD
Theatro
Therabody
ThermoPro
TIBO
Tile
Tomshine
Topesel
TopVision
Tracking Point
TRENDnet
Trust
TytoCare
Tzumi
UanTii
UBTECH
Ustellar
Vankyo
Vaultek
Veho
Velco
Venturer (RCA)
Vine
Vitamix
Vivint
Vivitar
Wattbike
Wattcost
Wearable X
WEBCATLY
Weber
WeeKett
Weenect
Weight Gurus (Greater Goods)
We-Vibe
Whirlpool
Whistle
Wimius
Winix America
Wsdcam
X10
XCOAST
Xiangshan
XODO (Contixo)
Xoopar
Xperi, DTS
X-Sense
Xueyu
Yeelight
YP
Yunmai
Zeeq
Zmodo Technology
X Rocker
iTime Jr.
Veho-lifestyle


www.iotsecurityfoundation.org

COPPER HORSE

www.copperhorse.co.uk

59-60 Thames Street, Windsor, Berkshire, UK, SL4 1TX
+44 (0) 208 1337 7337 @copperhorseuk