IoT Security Foundation

The State of Vulnerability Disclosure Policy Usage in Global Consumer IoT in 2025

A report prepared by Copper Horse Ltd
Published January 2026

Authors
Rohan Panesar, Mark Neve,
Ryan Baldwin & David Rogers

Contents

Foreword

Each year, this report charts the evolving maturity of security in the IoT ecosystem — and in its eighth edition, the direction of travel is clear.

The trend continues upward, with more manufacturers adopting structured vulnerability disclosure processes than ever before, yet progress remains slower than the pace of regulatory and technological change might suggest. The industry has learned much over eight years of this unique data series, but the gap between compliance and commitment persists.

The general pattern shows improvement in disclosure transparency, particularly among brand-name manufacturers and retailers who have embraced security as a value signal. UK retailers, in particular, stand out once again, with several achieving full compliance on sampled products — proof that clear domestic regulation can deliver tangible results. Elsewhere, movement remains uneven, with some manufacturers still treating disclosure as a checkbox exercise rather than an ongoing obligation.

This year's data highlights emerging patterns in how vulnerability disclosure is being implemented. More companies are referencing regulation directly, some formalising practices under Coordinated Vulnerability Disclosure (CVD), while others use third-party platforms or proxy services to manage reports. Regional differences are softening as legislation converges globally, but smaller vendors and newer market entrants still lag far behind public expectations.

The regulatory landscape has gathered pace and continues to tighten. In particular, the EU's Cyber Resilience Act extends the boundary of traditional vulnerability reporting to include the authorities – even in consumer sectors. This marks a distinct shift in legislative oversight. This will raise eyebrows, and the tension between regulatory intent and the traditional norms of industry practice will likely shape the next phase of industry discourse.

A more subtle trend gaining attention is found not in the manufacturers but in the channels of sale. The arrival of influencer-led commerce platforms, such as TikTok Shop, could reshape how IoT products reach consumers to some extent and may pose new oversight challenges for market surveillance authorities. These evolving ecosystems blur traditional accountability lines and will demand new thinking from regulators.

So while the headline indicators show encouraging movement, the story beneath remains mixed. Industry awareness has matured, adoption is climbing, but full alignment with global best practice is still some way off. This report remains the only data series of its kind capable of showing these longitudinal trends in clear relief — a valuable barometer for policymakers, practitioners, and consumers alike.

Congratulations once again to David Rogers and the Copper Horse team for sustaining this longitudinal research and continuing to shed light on where the sector is improving and where it must do better. As ever, the IoT Security Foundation's IoT Security Assurance Framework — boosted in 2025 (see af.iotsf.org) — and associated best practice materials, including guidance on vulnerability disclosure, remain central resources for improving secure design and responsible product stewardship. I commend this report to the reader.

John Moor, Managing Director, IoT Security Foundation

Executive Summary

This is the eighth report in a series tracking the adoption of vulnerability disclosure amongst manufacturers of internet connected devices. It is the second report since the UK's Product Security and Telecommunications Infrastructure (PSTI) Act regulations came into force in April 2024.

In addition to UK regulations, Australia has published the Cyber Security (Security Standards for Smart Devices) Rules 2025 along with upcoming regulation from the European Union – the Cyber Resilience Act (CRA) 2024 and the United States – FCC IoT Cybersecurity Labelling Program. All of these require IoT manufacturers to have a means for security researchers to contact manufacturers to report vulnerabilities in a coordinated manner. Other countries are adopting similar policies, in some cases voluntary.

The 2025 report added 68 new manufacturers of popular product showing that the IoT space is still expanding, however of these new entries into the market only 16/68 (23.53%) had a vulnerability disclosure policy with the vast majority 52/68 (76.47%) having no vulnerability disclosure policy. 35 manufacturers were removed from the list, either due to stopping selling devices in this space, or their product websites being no-longer accessible.

This headline figure for this year's report is that 40.53% of global IoT manufacturers have a way for security researcher to contact them. This means that 59.47% of all manufacturers do not. This figure is however an improvement of 4.94% on the 2024 report at 35.59%.

One area where improvements are visible and demonstrably beneficial to the public is in the retailer dip test. A sample of 15 popular vendors were captured from retailers to give a prospective idea of the level of exposure that end users had to potentially insecure products without manufacturers supporting vulnerability disclosure policies. In 2025, almost across the board there was an improvement, with all retailers seeing over 60% of popular manufacturers with a vulnerability disclosure policy. Additionally, nine of the 15 retailers sampled scored over 80%, and three UK retailers had 100% adoption among the popular IoT manufacturers' products they sold.

What is Vulnerability Disclosure?

Vulnerability disclosure is a best practice concept that grew out of the hacking community, which advocated for better ways to solve product and service vulnerabilities, without security researchers being threatened. At the same time, to ensure that the issues were actually fixed by companies, with users protected from potential threats by malicious actors. This process was eventually formalised into vulnerability disclosure. The concept of vulnerability disclosure has now been adopted by governments and industry and is internationally standardised. 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"[1].

Coordinated Vulnerability Disclosure (CVD) is the industry (and government) accepted best practice for vulnerability disclosure. There is coordination between the reporting researcher and vendor company until a resolution is reached, and the vulnerability is disclosed publicly. This typically involves notifying the manufacturer of the issue and providing a report, which is generally acknowledged within 24-48 hours. This acknowledgement and further communication keep the researcher informed of the resolution progress and allows for an open line of communication for the vendor to confirm details or request more information. The resolution time depends on the severity of the vulnerability but is often between 30 and 90 days, where a patch is released (if the issue is fixable with a software update). If the manufacturer does not resolve the issue, researchers face a dilemma: keep the vulnerability a secret and potentially leave devices insecure, reach out to industry or government bodies for assistance, or disclose publicly without the agreement of the manufacturer. A core tenet of CVD is that the vulnerability is publicly disclosed following resolution and agreement by both the reporter and vendor. The publication is something that may be done by one or both of the reporter and affected vendor. This disclosure may occur via a blog, social media, academic paper, or at a conference.

In recent years, the larger hacking conferences require that researchers have taken reported any vulnerabilities via a CVD process with any affected companies before the security research may be discussed at the event. This process ensures that companies have adequate time to fix the vulnerability and issue any patches to products before the issue is made public so that products are not exposed to exploitation by malicious actors.

The benefit of following a CVD process is that issues can be caught early, using a method that security researchers understand and endorse, meaning that end users and customers are ultimately better protected. With multiple pieces of legislation around the world requiring companies to implement a vulnerability disclosure policy, it is now more important than ever that IoT manufacturers create and one and actively use it. Table 1 contains free resources to get started:

Table 1
Vulnerability Disclosure Resources

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://www.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

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

Regions Retailing IoT Products

At the start of this research in 2018, the researchers created a list of popular retailers from around the world, where individuals would purchase consumer IoT products. This list of retailers is the foundation of the data gathering portion of this research and, in legislation, are bearing increasing responsibility for stocking compliant product. The retailer list has been reviewed once again to ensure included companies are representative of all regions of the world:

- 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 8th year of the report. Copper Horse first started investigating this topic in 2018, looking at the state of adoption of vulnerability disclosure among popular consumer IoT product manufacturers.

Vulnerability disclosure is one of the few publicly available indications of a company's security posture – a policy is either accessible online, or it is not. Copper Horse considers the lack of these policies as 'insecurity canaries' as it is one of the very few ways of measuring a company's poor stance towards security. Just as a canary would detect noxious gases in mines, looking at the lack of existence of a public vulnerability disclosure policy gives an early warning of concerns about cyber security.

As this research continues year-on-year, companies are lost from the dataset either because they cease operating or stop selling connected devices. This year is no different and that information is captured as part of the research.

The report generally uses the term vendor and manufacturer interchangeably. Retailers used to gather data are all popular retailers in their own geographic region, with an online store presence.

The methodology used in previous reports continues with this year's report. When the research began, a list of popular global retailers was created. This has expanded in previous reports to distributors in EMEA, APAC, NA, and LATAM for a better representation in these regions. The dataset is created (and expanded) by using the retailer's "Best Seller" metric in relevant categories to find the current popular IoT products. These manufacturers are then added to the dataset.

In previous reports, assessing Amazon and AliExpress posed a difficult challenge to the researchers due to the extensive list of products on those sites. This year the decision was taken to define a more refined method for data gathering on Amazon and AliExpress. As these websites are sprawling and have so many products listed, combined with an extensive number of categories, it is difficult to gather products using the existing methodology. A systematic sampling approach has therefore been taken. Using the product categories from the report, combined with the key words "Smart", "Connected", or "Wi-Fi" to augment the 'Best Seller' metric on these search queries gives a new way to gather the data for the report from this type of retailer.

With retail sales methods evolving and with the rise of new marketplaces, the methodology used may in future reports be fine-tuned. Firstly, to refresh the retailers list to include sellers such as Temu, due to its recent, significant gain in market share. In addition to this, emerging sales platforms such as TikTok Shop marks a departure from traditional websites selling products to consumers. Instead, an influencer promotes the product and provides a link to purchase the item in exchange for commission on the sale. This is a completely different way of selling products allowing manufacturers to directly reach consumers without needing to have a retail website or store, akin to a digital form of 'door-to-door' sales. This is likely to add another layer of difficulty for future retail and IoT security regulation.

Data Exception: Qardio

A manufacturer of connected health monitoring products, Qardio, was found to have ceased operating after the research window had closed and towards the end of the report writing phase. Upon further investigation, it appears that the organisation stopped shipping products sometime in the latter half of 2024, however the website remained active and, according to some forum posts and Trustpilot reviews, the company were still accepting orders and taking payments until August 2025.

The reason for the closure is not clear, as the company has not released a statement, but it should be noted that multiple vulnerabilities were discovered[2] in both the company's iOS and Android heart health monitoring apps, along with vulnerabilities in their blood pressure monitoring device. This change will be addressed in the 2026 report.

2. https://cyberinsider.com/zero-day-flaws-found-in-qardio-heart-health-ios-and-android-apps/

Key Findings

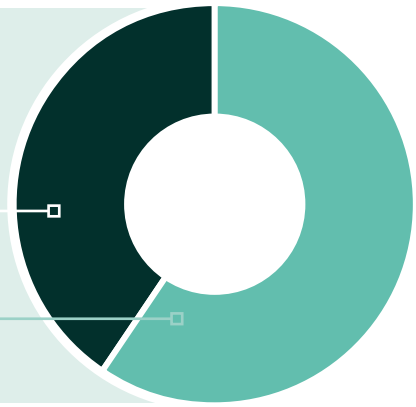
The 2025 research has found that 199/491 (40.53%) of the IoT manufacturers in the dataset have a method for security researchers to contact them about a security vulnerability. This is a 4.94% increase on the data from 2024. This year's continues the general trend observed in previous reports. There are currently 59.47% of manufacturers that still do not have a way for security researchers to contact them.

Figure 1

The Headline Figure

40.53% of the companies had a way for security researchers to contact them.

59.47% of the companies didn't have a way for security researchers to contact them.

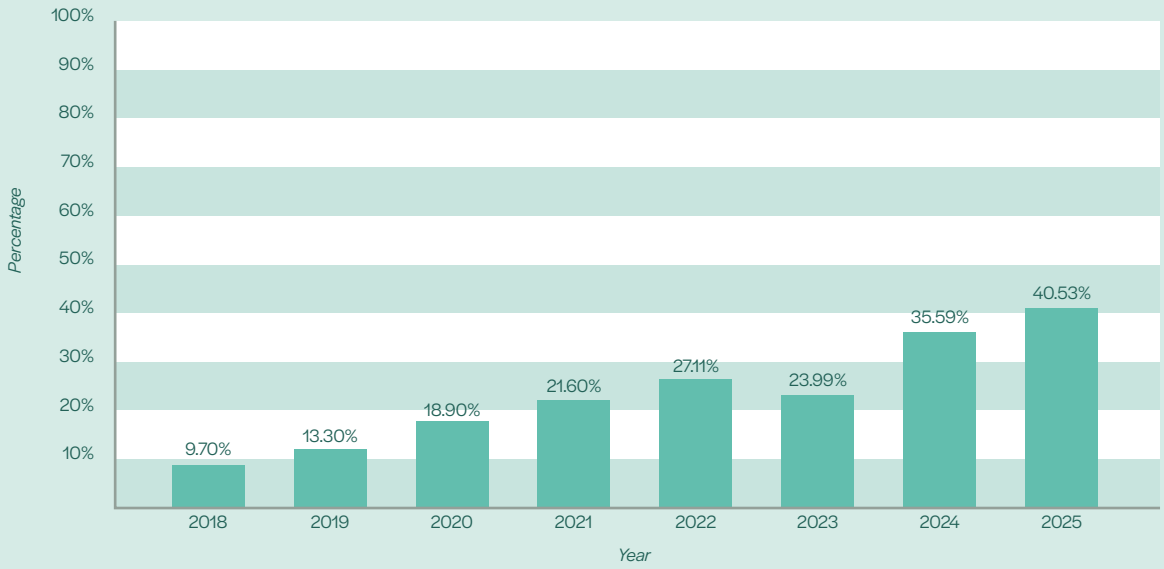


The overall dataset changes year-on-year as vendors cease operating or stop selling connected devices. In 2025, the dataset now consists of 491 vendors, with 35 companies being removed and 68 newly added manufacturers.

Figure 2 displays the year-on-year headline figure since this research commenced seven years ago.

Figure 2

Year-on-Year Trend



Predicted Trend Discussion

The seven previous years of this report have given the researchers a lot of data to predict the future trend. In 2024's report, 100% adoption was projected to be achieved in 2045. Figure 3 is a line graph showing measured adoption of policies from previous reports, with the dashed line indicating the forecasted growth of adoption. While adoption levels have improved over time, they remain slow. These new figures point to an increased adoption rate, bringing the target of total adoption closer by 5 years. At the 2025 report rate of adoption, it will take until approximately 2040 to achieve full coverage.

At the 2025 report rate of adoption, it will take until approximately 2040 to achieve full coverage.

Looking back at previous predictions from this report, which started in 2022's report, the figure for 2025, based on extrapolation was expected to be slightly short of 40%. 2023 saw a correction as the dataset was significantly expanded, with the predicted 2025 adoption being less than 35%. The 2024 report saw a similar value. Tracking the original 'core' dataset of IoT manufacturers in those two reports saw the same figure as 2022's prediction – just short of 40% at 2025. It could therefore be a reasonably confident prediction that 2026's headline figure of adoption will be around 43%, with 57% of manufacturers still to adopt any form of vulnerability disclosure policy.

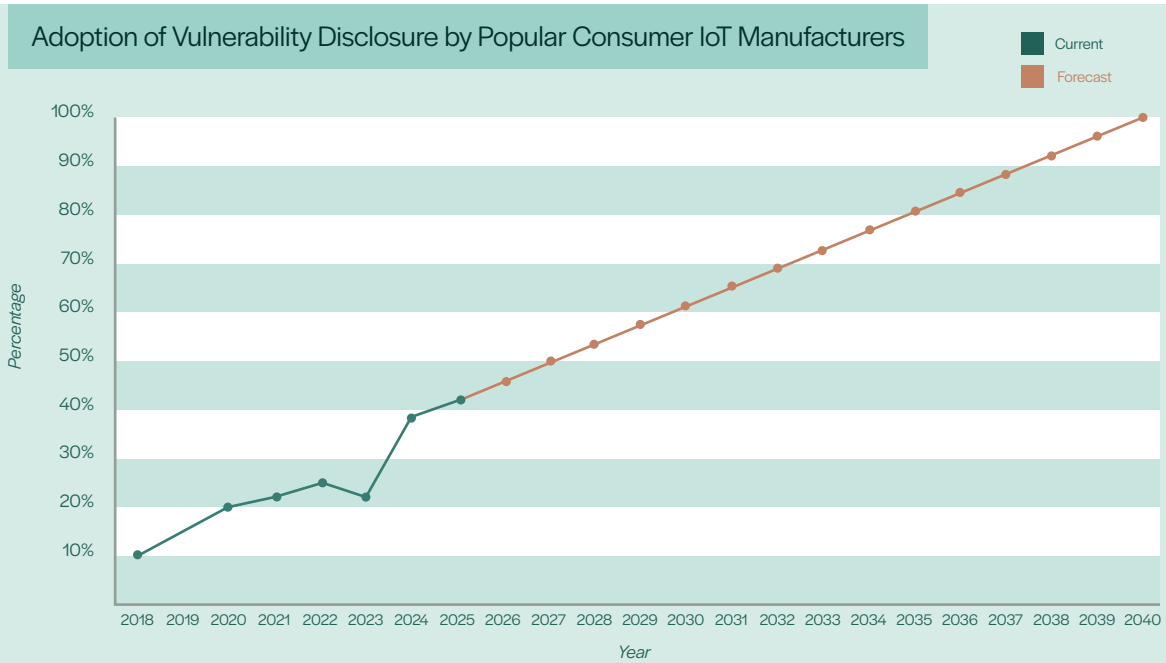
The incoming Cyber Resilience Act (CRA) across Europe is likely to cause a significant increase in adoption as companies are required to meet basic requirements for vulnerability disclosure in 2026.

All of this must be caveated by the fact that the future is not likely to see organic growth of this figure. The incoming Cyber Resilience Act (CRA) across Europe is likely to cause a significant increase in adoption as companies are required to meet basic requirements for vulnerability disclosure in 2026. Further information on this is contained in the Global IoT Policy section later in this report.

As with previous reports – the entire dataset is available as open data on the Copper Horse website[3].

Figure 3

Adoption of Vulnerability Disclosure by Popular Consumer IoT Manufacturers



3. https://copperhorse.co.uk/iot-vulnerability-disclosure-research/

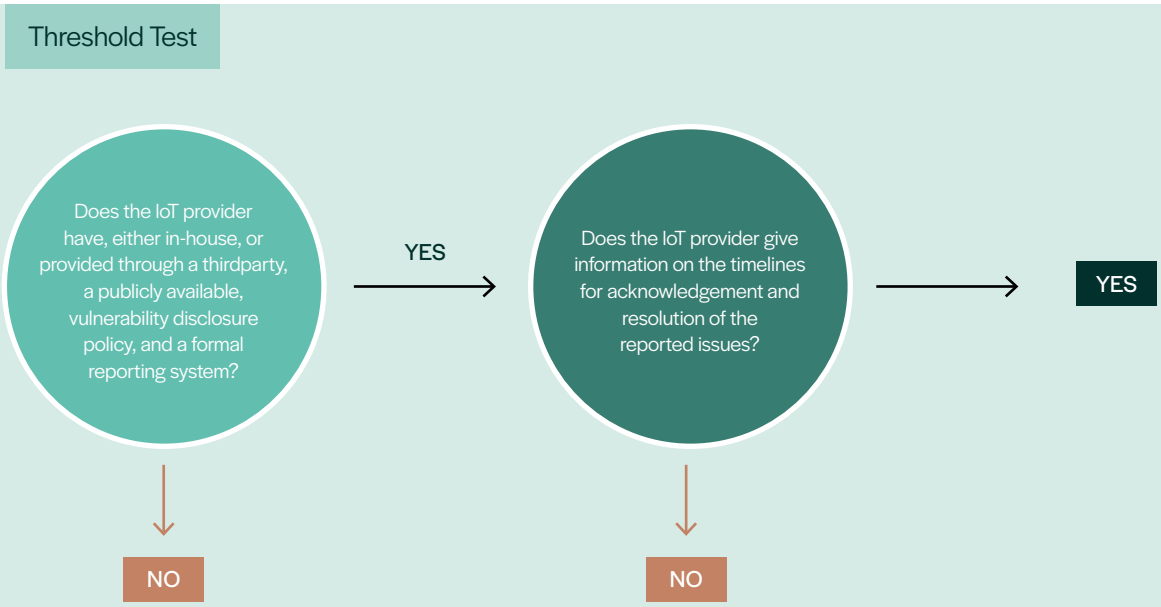
Threshold Test

In 2020 the researchers of this report established a threshold test to provide statistics on vendors' vulnerability disclosure implementation. The basis of the threshold test is the UK's PSTI Act requirements related to vulnerability disclosure.

The test is comprised of two parts:

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

Figure 4



A full list of the manufacturers that met these threshold tests is listed in the Annex of this report, indicated in green for those that passed both parts of the test, amber for those that only passed one part and red for those that failed both.

The table below shows the overall results:

Table 2
2025 Threshold Test Results

Test	Number of Manufacturers	(%)	Change from 2024
Passed both parts of the threshold test	136/491	27.70%	↑ 6.25%
Passed only one part of the threshold test	63/491	12.83%	↑ 1.58%
Failed both parts of the test	292/491	59.47	↓ 4.94%

Threshold Test (cont.)

Overall, there has been an increase in the number of manufacturers compliant with legislation that requires organisations to both have a policy & provide information on expected timelines. This year the research found that 136/491(27.70%) of the manufacturers in the dataset passed both the first and second parts of the threshold test, an increase of 6.52% on 2024. 2024's research saw a significant increase, over double that of the previous 2023 figure. This may have been due to the requirements of the UK's PSTI Act coming into force in April 2024.

In 2025, the research captured multiple vendors implementing a policy which previously had not had one – with some even making direct reference to PSTI. The table above shows that the general movement is towards compliance, with those failing to pass the test still representing the lion's share of the data. With the UK's PSTI Act regulations in place and some of the EU CRA's basic requirements coming into force in 2026, it was expected that there would be a greater increase in the numbers of organisations meeting one or both parts of the Threshold Test.

34 manufacturers moved up in category since the last report, with 20 of those moving up from the red category to green, 10 from amber to green and 4 from red to amber.

For manufacturers that had moved down categories, 3 manufacturers moved from amber to red: Rachio, Ruark and Tefal. Two – Yamaha Pro Audio and Yamaha Corporation moved from green to red.

Examining Retailer Compliance

Both the UK's PSTI Act and the EU's CRA not only focus on manufacturers but also require distributors and retailers of connected devices to ensure compliance when it comes to stocking products. This report introduced a 'dip-test' in 2022 to gauge retailer compliance across different regions. This test involves researchers visiting the retailers used for this research and gathering the top connected product manufacturers stocked on each one, now capped at 15 (or as many as is stocked if under that number), then establishing whether these manufacturers have adopted vulnerability disclosure.

Three UK retailers, Currys, John Lewis, and Argos were all found to have 100% vulnerability disclosure support among the manufacturers of popular devices

When this dip-test was initially established, the UK, US, and EU were chosen as these regions had the most movement in the IoT security regulation space. This broadly remains the case – the research has therefore analysed the same regions for 2025. For the UK, the retailers Smyths Toys and Tesco were also used for the dip-test. These two are important since Tesco is the largest supermarket chains in the UK, and Smyths one of the largest toy retailers. It is a prime retailer of smart products targeted at children, an area that has historically seen poor security and impactful hacks. It should be noted that Tesco does not have a mechanism to sort by popular products, so data was gathered from its smart product categories, without sorting by a popularity metric.

The results in 2025 for retailers Europe and the US were very similar with 35/45 (77.78%) and 58/75 (77.33%) – with both showing significant increases on 2024's figures. Europe's increase was just over 16% (from 2024's figures of 43/70 (61.43%)) and the US was a 32% increase from 2024's figures of 29/64 (45.31%). The UK saw a similar increase to Europe of nearly 17% from 2024's number which was 55/75 (73.33%), reaching 70/81 (86.42%) products for which the manufacturers had vulnerability disclosures.

Table 3 shows the retailers used in this dip-test.

Table 3
Retailer Compliance

Region / Country	Retailers	Manufacturers Using Vulnerability Disclosure 2024	Manufacturers Using Vulnerability Disclosure 2025
USA	Walmart	8/29 – 27.59%	11/15 – 73.33%
	Best Buy	13/23 – 56.52%	13/15 – 86.67%
	Target	8/12 – 66.67%	11/15 – 73.33%
Europe	Cdiscount	6/12 – 50.00%	12/15 – 80.00%
	ePrice	6/11 – 54.55%	12/15 – 80.00%
	El Corte Ingles	12/17 – 70.59%	12/15 – 80.00%
	Otto	11/20 – 55.00%	10/15 – 66.67%
	Media Markt	8/10 – 80.00%	12/15 – 80.00%
UK	Amazon UK	7/15 – 46.67%	9/15 – 60.00%
	Currys	10/15 – 66.67%	15/15 – 100.00%
	John Lewis	14/15 – 93.33%	15/15 – 100.00%
	Argos	13/15 – 86.67%	15/15 – 100.00%
	Tesco	9/10 – 90.00%	11/15 – 73.33%
	Smyths Toys	2/5 – 40.00%	5/6 – 83.33%

Examining retailer compliance (cont.)

Across the board there has been a notably positive increase in the stocking of manufacturers that support vulnerability disclosure. Three UK retailers, Currys, John Lewis, and Argos were all found to have 100% vulnerability disclosure support among the manufacturers of popular devices. Smyths Toys saw a significant improvement, doubling manufacturer adherence over 2024, although against the low number of smart products that they stock. The US's Walmart saw the largest increase of nearly 46%, from 8/29 (27.59%) in 2024, to 11/15 (73.33%) in 2025. The lowest performing retailer was Amazon UK followed by Otto, with 9/15 (60.00%) and 10/15 (66.67%) respectively, but also an improvement on their previous years' figures.

These figures are a very positive signal that things are changing at the point at which consumers buy a product and it may indicate that the problems in the consumer IoT space now lie in the 'long tail' of the market.

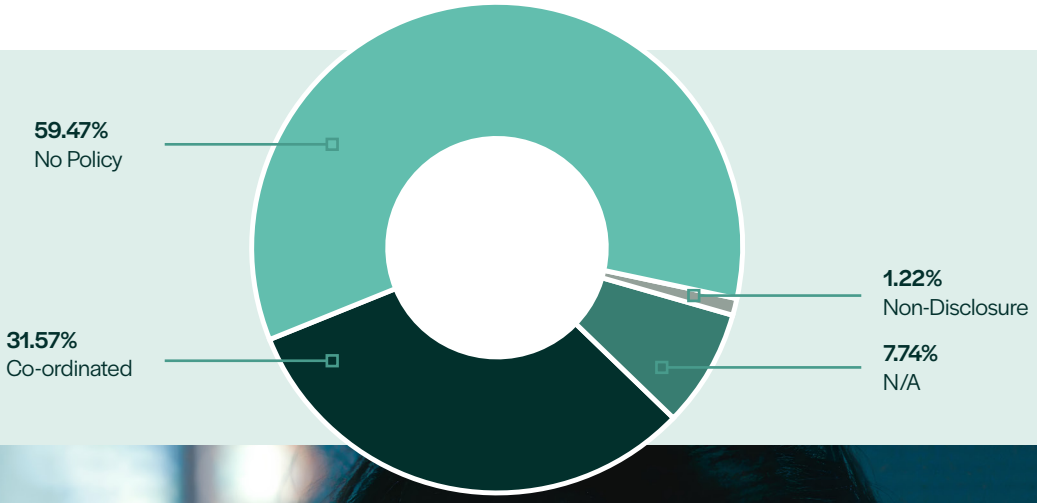
Overall, these figures are a very positive signal that things are changing at the point at which consumers buy a product and it may indicate that the problems in the consumer IoT space now lie in the 'long tail' of the market, which may represent significantly less sales volume.

Types of Vulnerability Disclosure

There are various forms of vulnerability disclosure, but Coordinated Vulnerability Disclosure (CVD) is the industry best practice and internationally standardised form of vulnerability disclosure, where security researcher and impacted vendor work together to identify, triage, resolve, and coordinate a public disclosure of the vulnerability.

The research from 2018 up until 2025 has always shown that the majority of manufacturers in the dataset with a policy, use CVD. In 2025 this figure was 155/199 (77.89%), an increase of nearly 5% on 2024's 119/163 (73.00%). Looking at the dataset in its entirety, CVD represented 155/491 (31.57%). While CVD is used by over 77% of the vendors in the dataset, 6/199 (3.02%) of those that used a policy or 6/491 (1.22%) of the overall whole still explicitly outline non-disclosure policies. The remaining vendor policies are not clear whether the process would be in line with CVD and are marked as such in the dataset; these represent 38/199 (19.10%) of those that had some kind of vulnerability disclosure or 38/491 (7.74%) of the overall whole.

Figure 5



Regional Differences

As has been seen in the previous reports in this series, the majority of the manufacturers in the dataset are headquartered in North America, Asia, and Europe, with 177, 165 and 129 respectively. This is followed by a much lower number of six manufacturers from Oceania and five from South America. The remaining nine vendor headquarters were not possible to locate as the information was unavailable. Some of these companies do not even have a website.

Europe had always lagged behind but now slightly leads the world regions in vulnerability disclosure adoption

In 2024, the dataset included four generic wearable manufacturers headquartered in Africa. In 2025, these vendors had either stopped selling connected devices or ceased operating. They have therefore been removed from this year's report.

The data in 2025 shows an interesting trend. All three of the regions that dominate the dataset (Europe, North America, & Asia) have seen an increase in the manufacturers headquartered in the region adopting vulnerability disclosure practices.

Prior to 2024, Europe had always lagged behind but now slightly leads the world regions in vulnerability disclosure adoption, with an increase of 6.68%, from 47/118 (39.83%) in 2024 to 60/129 (46.51%) in 2025. North America is second with 80/177 (45.20%), up from 65/173 (37.57%) and Asia following closely behind with 57/165 (34.55%), increasing from 50/147 (34.01%) in 2024. As mentioned above, vendors headquartered in South America and Oceania are not largely represented in the dataset but of these, there is only one manufacturer in each territory that supports vulnerability disclosure practices: 1/5 (20%) in South America, the same figure as in 2024, and 1/6 (16.67%) in Oceania, increasing from 0/6 (0%) in 2024.

Product Categories

These product categories or segments represent the primary type a vendor produces. While manufacturers in the dataset often produce a wide range of devices, the primary product category allows for analysis of the different levels of adoption among popular connected product verticals.

Generally, the categories in 2025 all outperformed the 2024 report's findings. The exceptions were the Smart Lighting and Hub category which remained the same and the Audio and Mobile categories where there was a decrease of around 5%. Table 3 outlines the level of adoption in each category.

Table 4
Product Category Adoption

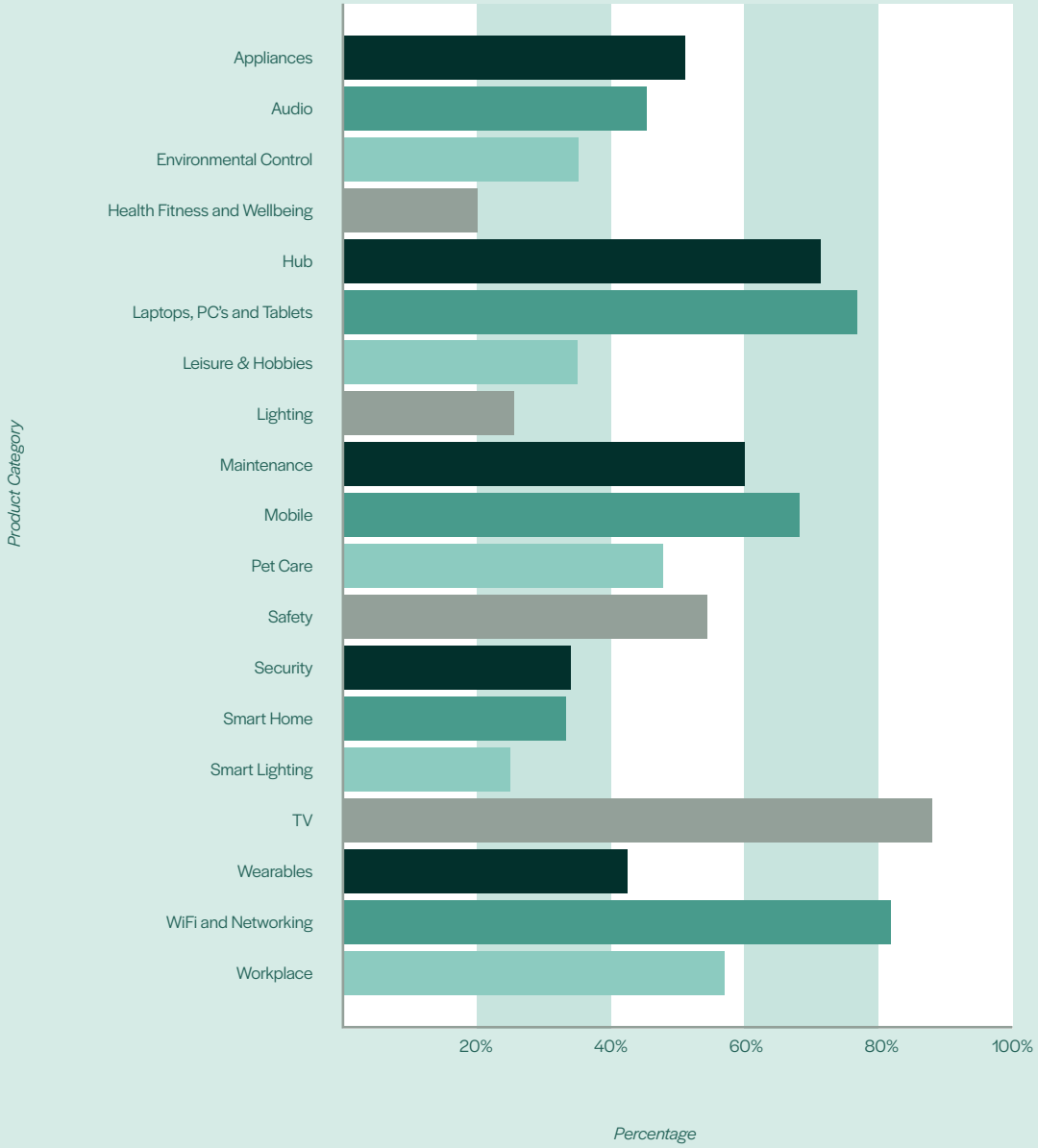
Retailer	Number	%	VS 2024
Appliances	18	51.52%	↑
Audio	10	45.45%	↓
Environmental Control	7	33.33%	↑
Health Fitness and Wellbeing	8	20.00%	↑
Hub	3	75.00%	–
Laptops, PCs and Tablets	7	77.78%	↑
Leisure & Hobbies	2	33.33%	↑
Lighting	13	25.49%	↑
Maintenance	3	60.00%	↑
Mobile	11	68.75%	↓
Pet Care	5	45.45%	↑
Safety	5	55.56%	↑
Security	30	32.97%	↑
Smart Home	26	32.50%	↑
Smart Lighting	1	25.00%	–
TV	7	87.50%	↓
Wearables	21	43.75%	↑
Wi-Fi and Networking	13	81.25%	↑
Workplace	10	58.82	↑

Improved on 2024 figures Same as 2024 Worse than 2024

Product Categories (cont.)

Figure 6

Product Category Vulnerability Disclosure Adoption



Enterprise

Since 2021 this research has tracked a selection of Enterprise or Business-to-Business (B2B) companies to observe how these vendors differ from consumer IoT. The findings of this dataset are static, with 44/48 (91.67%) of enterprise IoT manufacturers having a vulnerability disclosure policy, noting that no new companies were added to this dataset in 2025 and that it is not the primary domain of this report. It is noted that the UK government ran a Call for Views on enterprise connected device security in the summer of 2025. The results were not yet published at the time of writing this report[4].

Proxy Disclosure and Bug Bounties

Organisations exist that facilitate vulnerability disclosure policy creation and maintenance as well as coordinating the other parts of the process. In this report, these are referred to as proxy disclosure companies. Some manufacturers may choose to defer responsibility for vulnerability disclosure to these organisations simply because they don't have the resources to maintain the disclosure / management process. Others, that as a business decision, they would rather host a policy through a proxy organisation.

This research has throughout its time noted some vendors choosing to use a vulnerability disclosure submission form provided by one of the proxy disclosure companies, embedded within the vendor's website, to take submissions from security researchers. In 2024, 34/458 (7.42%) of the dataset's manufacturers used proxy disclosure. There was a small increase in this number in 2025 with 39/491 (7.94%). In 2025, BugCrowd and HackerOne were the dominant organisations with 18/39 (46.15%) and 18/39 (46.15%) manufacturers using them. This was followed by Intigriti and Yes We Hack with 2/39 (5.13%) manufacturers each. In 2023, the research captured another proxy organisation, BugBase, but the company has not been represented in the data since.

Table 5
Proxy Disclosure Organisation Usage

Organisation	2024 (%)	2025 (%)
Manufacturers not using proxy disclosure	423/458 (92.36%)	452/491 (92.06%)
BugCrowd	16/458 (3.49%)	18/491 (3.67%)
HackerOne	16/458 (3.49%)	18/491 (3.67%)
Intigriti	1/458 (0.22%)	2/491 (0.41%)
Yes We Hack	2/458 (0.44%)	2/491 (0.41%)

Some manufacturers choose to use a financial reward to incentivise security researcher participation. This mechanism is usually called a Bug Bounty. According to a report[5] published by ENISA, financial rewards have been found to be one of the most effective methods of incentivising security researchers. Similar to a vulnerability disclosure policy, bug bounties often include the scope for submissions that will be accepted and usually contain payment information depending on the severity of the vulnerabilities / exploits that are submitted. In 2025 a minimal increase in the usage of such schemes was captured, rising by six manufacturers to 44/491 (8.96%) from 38/458 (8.30%) in 2024.

4. https://www.gov.uk/government/calls-for-evidence/call-for-views-on-enterprise-connected-device-security
5. https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure

Use of /security pages and Use of security.txt

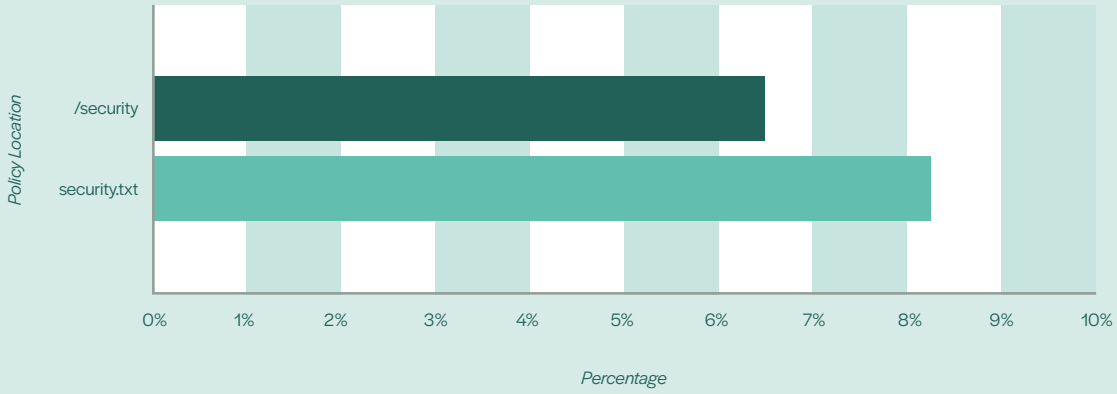
This research has tracked two possible locations of vulnerability disclosure policies on vendor websites, these being: on a /security page or at /.well-known/security.txt. The former is a recommendation in the IoTSF Vulnerability Disclosure Best Practice Guidelines, and the latter is an initiative to make a company's security policies easier to discover by security researchers. These however are not the only locations to find vulnerability disclosure policies. Both of these locations have seen a slight increase in usage in 2025, with /security increasing from 26/458 (5.68%) in 2024 to 34/491 (6.92%) in 2025.

Security.txt usage has increased by a similar proportion, from 36/458 (7.86%) to 44/491 (8.35%). Three of the vendors using security.txt are also captured in the data as not having a vulnerability disclosure policy. This is because these companies do not have a policy to speak of – the security.txt file simply contains a contact email address, without a link to a policy, which often included in the file.

Another interesting observation is that many of the new adopters of vulnerability disclosure in the 2025 research seemingly do not use either /security or .well-known/security.txt. These companies may be adopting a policy to comply with the PSTI Act or other similar legislation; noticeable by a specific mention to the legislation or the policy being stored in the vendor's legal compliance section of a website. This is something that may be investigated further in future reports.

Figure 7

/security & security.txt Adoption



Pretty Good Privacy (PGP) Keys

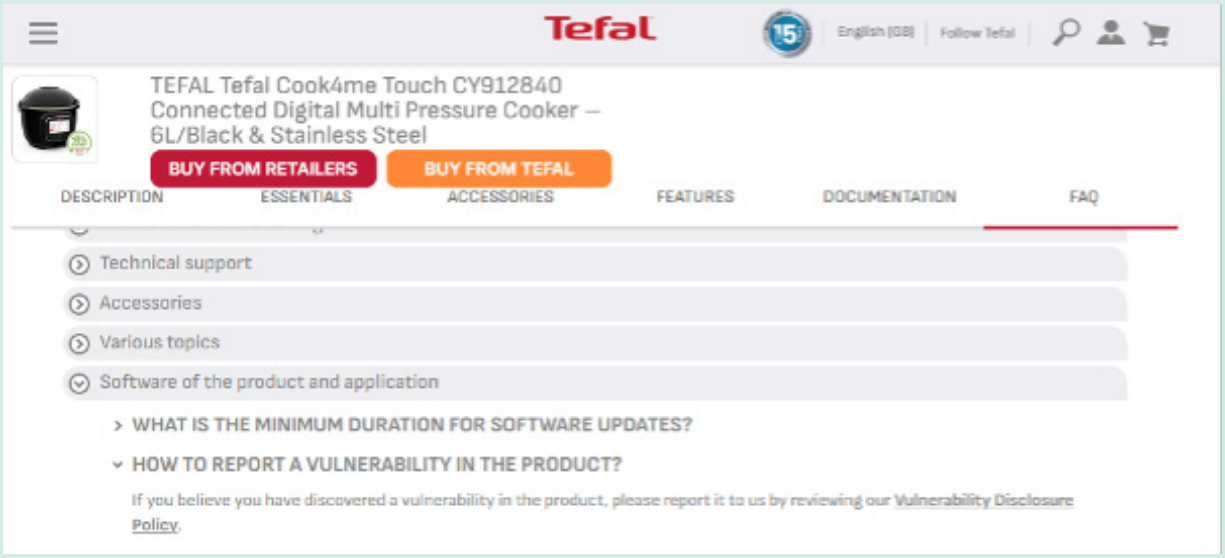
Companies using vulnerability disclosure may choose to allow submissions to be encrypted using PGP (or similar). In 2025 the percentage of the dataset using PGP keys for submission has only slightly increased, with 71/491 (14.46%), from 2024's 65/458 (14.19%). The reason for the lack of increase may be due to vendors tending towards using secure web forms, some of which are provided by proxy disclosure organisations – this is a feature that may be tracked in future reports.

Observations and Talking Points

Tefal

Tefal, who are owned by Groupe Seb, have previously had a vulnerability disclosure policy. This was located at https://vdp.groupe-seb.com/. Despite being included in Tefal product manuals, in 2025 this link was found to no longer load. Upon further investigation it seems that Groupe Seb may have ported parts of its website to the URL https://www.groupeseb.com/. After scoring an amber in the threshold test for the first time in 2023, Tefal's threshold test score has been relegated back to red, as clicking the link to their vulnerability disclosure policy returns a 404 'not found' error.

Figure 8 Tefal Product Information Including Vulnerability Disclosure Information

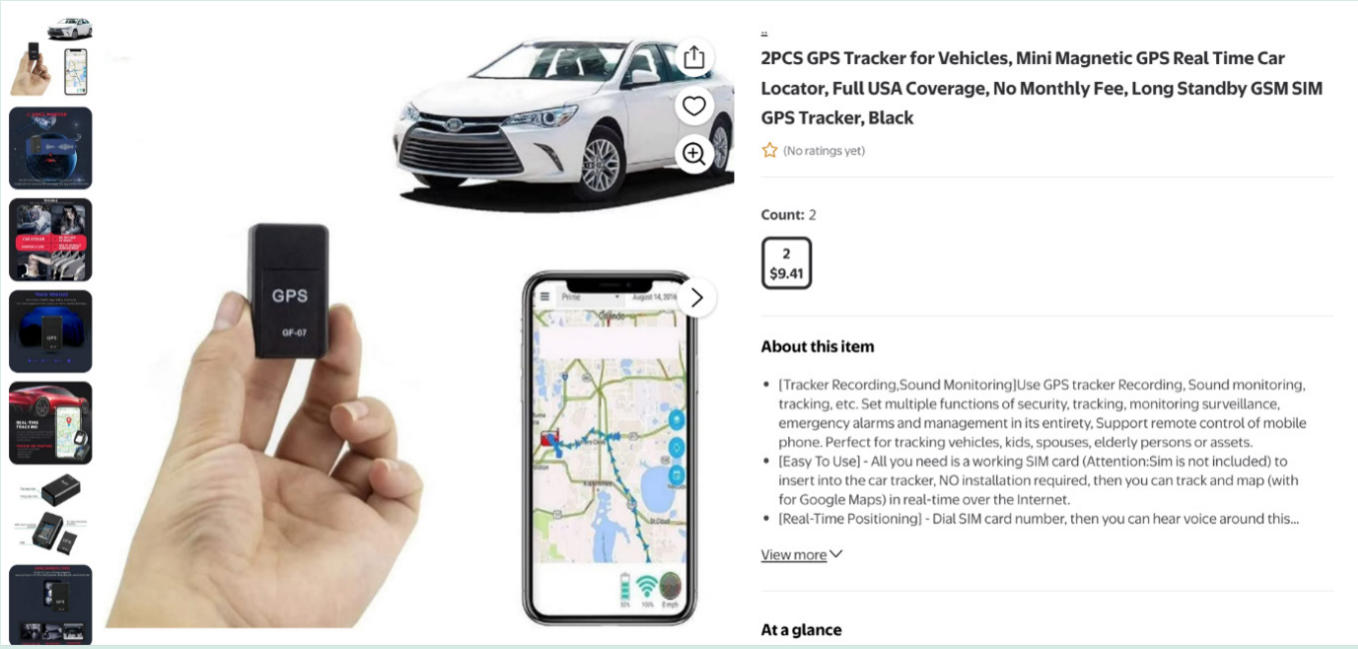


Walmart

During the research window for 2025, Walmart's retail website was again used to collect data on the connected products they sell. Two interesting products were observed in this process. The first being a product that seemingly had no brand (see Figure 9), along with a second, different brand, 'Teewix' that when investigated did not appear to sell connected devices but instead sold trousers. Since the research phase concluded, the product has disappeared from the Walmart website and the Teewix website no longer loads.

These two examples are indicative of a larger problem, connected devices with difficult to discern brands and manufacturers. The first, brandless device, sold as a 'GPS Tracker for Vehicles', a device that could in theory collect very sensitive data. It is difficult to discover whether the manufacturer of a device without a brand name, website, or any presence online is compliant with relevant legislation, or for security researchers to report any kind of issue to the manufacturer.

Figure 9 Walmart 'No-Name' GPS Tracker Listing



Researcher Engagement

Having a vulnerability disclosure policy is only useful as a security mechanism if you have security researchers to engage with it. Historically there have been many cases where researchers have attempted to disclose a vulnerability to an organisation, only for the entire process to backfire on the researcher, resulting in threats of lawsuits. One example that illustrates this well is the 2018 One Planet Yorkshire app incident[6] – involving a local council's app in the United Kingdom. The app was used to check bin and recycling collection dates. A security researcher discovered that while using the app, navigating to a certain page would allow the researcher to view other users' personal data. This researcher reached out to the City of York Council to disclose the vulnerability, following the Council's advertised vulnerability reporting programme. The Council announced a data breach, due to "deliberate and unauthorised access by a third party" and reported the researcher to the police. They claimed they could not contact the researcher following their report, but this was not the case as later evidenced in the researcher's public report. Thankfully, North Yorkshire Police concluded the developer was not in breach of the Computer Misuse Act, after the Council had reported the incident as such. The app was later removed from the app store, and the Council revised their statement, calling the vulnerability report "well intentioned". Despite having a vulnerability disclosure policy and programme, this situation shows what can occur when the process is not understood by the organisation that hosts it.

As the knowledge of vulnerability disclosure has risen and security researchers are not immediately assumed to be malicious actors, situations as described above occur less often. Two positive stories drawn out of this report's research for 2025 were that of Starlink and Oppo. Both vendors encourage participation in their vulnerability submission processes, but in slightly different ways:

- Starlink has a document entitled "STARLINK WELCOMES SECURITY RESEARCHERS"[7], where it outlines in detail the security requirements and properties of the devices they produce, encourages security researchers to test its devices and report findings of concern to them. The document is written in a very friendly tone and actively encourages researchers to apply for a job in the Starlink security team as well as pointing to their bug bounty scheme.
- Oppo takes this a step further with its bug bounty scheme. At the time of research, the company was offering an event on its 'Oppo Security Center' site[8]. Security researchers submitting vulnerabilities would receive double points, which could be redeemed for rewards, as well as a "special gift". While pitched as a fun, competitive method of further incentivising security researchers, it may in fact benefit provide the opposite as it appears there is no financial bounty value publicly linked to the points. Security researchers may take the view that this is a form of exploitation of their labour.

Figure 10

OPPO SRC Bug Bounty Event

🎉 OSRC 7th Anniversary Bug Bounty Event! 🎉

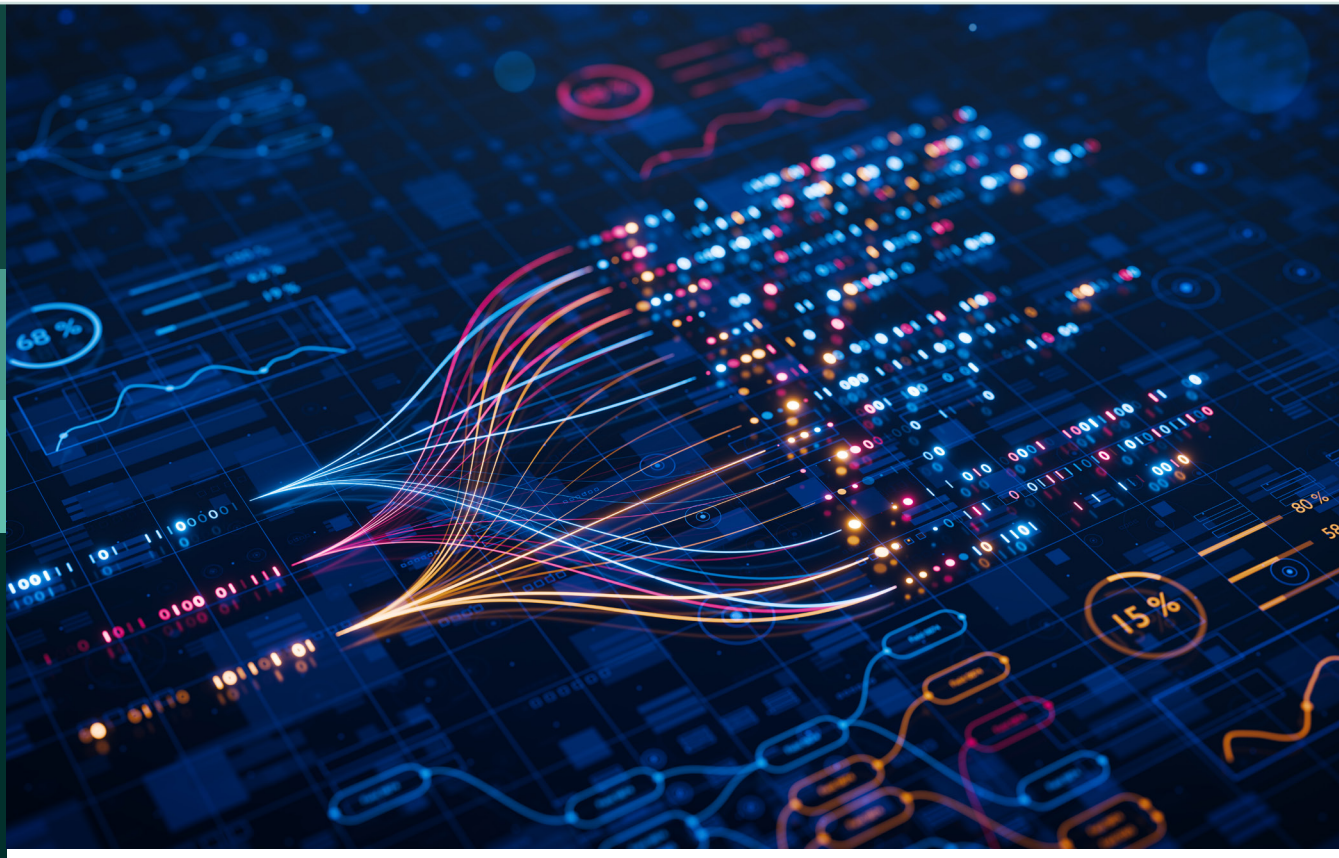
We are thrilled to celebrate 7 incredible years in the security community! To commemorate this milestone, we are launching a special Bug Bounty Event designed for all the hackers.

Event Details:

Duration: 2025/08/03 – 2025/08/30
Rewards: Earn DOUBLE rewards for targeting different scopes and levels!
Special Gift: Every participant who submits a valid report will receive a customized anniversary gift from OSRC!
This is a great opportunity for hackers to showcase your skills and earn prizes while helping to improve our security landscape. Whether you're a seasoned pro or just getting started, everyone is welcome to join!

Let's make this celebration memorable. Your contributions can make a real difference. Happy hunting!
Join us and let's find those vulnerabilities together!

6. https://www.rapidspike.com/blog/one-planet-york-data-breach-update/
7. https://www.starlink.com/public-files/StarlinkWelcomesSecurityResearchersBringOnTheBugs.pdf
8. https://security.oppo.com/en



Security.txt Issues

In the view of Copper Horse, the security.txt is a great initiative. In the context of IoT vulnerability disclosure, it gives manufacturers a unified location to store a vulnerability disclosure policy. It gives security researchers a common location across any website to search for relevant information.

This research has consistently encountered security.txt implementations that are not adherent to RFC 9116[9] – the IETF specification that outlines how to correctly implement security.txt. One of these requirements is that a security.txt file must have an expiration date and recommends that these not be more than one year in the future. This requirement is often overlooked. In 2025, during the research window, both BT and Tile (Life360) had expired policies – with Life360 having a security.txt that was almost three years expired at the time of research. Additionally, it appears that HP may have updated its vulnerability disclosure policy/policy location, as both the policy and encryption information were linked in its security.txt, but both links were broken and simply returned a 404 'not found' error. These issues may seem trivial but signals to a security researcher that the channel of communication and reporting process they are seeking out is not maintained.

9. https://datatracker.ietf.org/doc/rfc9116/

Security.txt Website Locations

During the research, as well as manually checking each website for a security.txt file to ascertain the file location, the report researchers also use an internal tool to automate the process of capturing the contents of the security.txt file. This tool also allows for a capture of a snapshot of the files on the day the tool is run, enabling any future changes to the security.txt file to be monitored.

Occasionally researchers find the vulnerability disclosure policy on a different website. This can sometimes be either the parent company of the manufacturer, or a group of companies which have a single contact point. An example of this is as follows:

- Netamo are part of the Legrand group. When navigating to the company's security page: https://www.netatmo.com/security-incidents , the site will redirect to: https://www.legrand.com//cybersecurity/en which helps by offering security researchers multiple paths to the disclosure policy. However, if researchers try to find the security.txt for Netamo on the manufacturer's own website at: https://www.netatmo.com/.well-known/security.txt the site returns a 404 error – page not found. The security.txt is located at: https://www.legrand.com/.well-known/security.txt but there is no redirect, making it more difficult to find the appropriate contact information, policy or PGP key.

This research also found sites using sub-domains and different internet top-level domains (TLDs) to host the security.txt file. For example:

- Products are sold at the website: deeper-sonar.com but the security.txt file is hosted at: deeper-sonar.sk

Although these companies provide all the details needed for security researchers to contact them, ultimately having the products hosted on a different domain to the security.txt file makes it more difficult to retrieve all the information when reporting a vulnerability and can slow down the remediation process, increasing the risk of vulnerabilities being exploited.

Another interesting find when validating security.txt files was the TP-Link implementation:

- when navigating to the security.txt URL, its implementation redirects users from: https://www.tp-link.com/.well-known/security.txt to TP-Link's security advisory page rather than providing a downloadable text file. Using the file downloading utility wget to retrieve the security.txt would download the html content of the webpage rather than the expected contact email address, .pgp key and link to the reporting template which a security researcher would require to contact the company to report the vulnerability.

All of these mis-implementations complicate the process of reporting vulnerabilities, however this may indicate the internal, big company challenges of implementing change across a large organisation with multiple business units. To help, there is an implementation guide available together with the IETF standard for security.txt.

Response Efficiency

The proxy disclosure company HackerOne provides “Response Efficiency” metrics on every policy that is hosted through its platform. These metrics give an indication of how a vendor handles reports, with time to respond (acknowledge report), triage, bounty (if applicable), and resolve. HackerOne also has the concept of “Healthy response times” which are recommended timelines for companies hosting through its platform. In 2025, researchers found that the fitness company Peloton had a response efficiency percentage of only 11%. This means that (during the research window of this report), Peloton only responded to 11% of disclosures within HackerOne’s recommended timelines. Similarly, the barbecue company Weber was found to have a response efficiency of 33%. These numbers can be seen as worrying because the longer a vendor takes to respond to a vulnerability report, the longer consumers are using a potentially insecure device. The flip side of this is that the transparency of this information allows for that problem to be addressed by the company and informs security researchers of what to expect. It is not known what type of vulnerabilities are being received by these companies either – a complicated hardware-related vulnerability for example can take a very long time to investigate and provide a fix for.

It remains a fact that a vulnerability disclosure policy is only useful as a security mechanism if it is maintained and that the process is faithfully followed by the company providing the policy, ensuring that vulnerability submissions are replied to and investigated in a timely manner.

Smart Watch Manufacturers

In 2025, the report researchers observed a change in the wearables market. In 2024, Fossil, a fashion brand that for some time was making smartwatches, made the decision to exit the market in order to return attention to their traditional business. Fossil Group also produced smartwatches for companies like Armani Exchange, Diesel, and Michael Kors, meaning these brands have also stopped selling connected wearables. The reasons for this shift are not entirely clear, with the Fossil Executive Vice President stating that "the smartwatch landscape has evolved significantly over the past few years, we have made the strategic decision to exit the smartwatch business". This change has occurred in the wake of increasing IoT security regulation, but this is unlikely to have been a major factor in this decision – there is fierce competition from smartphone manufacturers in the watch space, with connected products expertise that traditional watch manufacturers simply don't have.

Tick-box Compliance?

One observation on new adopters of vulnerability disclosure in this dataset is that their policies are often not located in traditional, easy to find places such as /security or /.well-known/security.txt. Many of these new adopters seem to have implemented vulnerability directly as a result of legislation like the UK's PSTI Act, such as Devialet and Weber. This report's researchers found these policies are sometimes stored in a legal compliance section of a site, or only discoverable through a search engine.

Global IoT Policy

Previous reports have tracked the movement by governments towards protecting consumers by enacting rules which require manufacturers to provide a minimum level of security for IoT products.

Some countries have chosen to make these rules voluntary, while others have passed laws mandating cyber security rules for devices. Many of these regulations are based on international standards such as ETSI EN 303 645[10] – 'Cyber Security for Consumer Internet of Things', and vulnerability disclosure guidelines – ISO/IEC 29147[11] – 'Security techniques – Vulnerability disclosure'. These standards require IoT manufacturers to manage cyber security from the design phase through development, launch and through the life of the product. Even though some countries have passed laws requiring manufacturers to have public disclosure policies, the data shows that manufacturers are still lagging behind on implementation. There are an increasing number of countries that have made both mandatory and voluntary requirements for vulnerability disclosure policies for connected product / IoT manufacturers, not least the entire 27 country membership of the EU. Note that there is also other legislation in domains related to IoT, such as the European NIS2 Directive that will require CVD adoption.

Australia

The Australian government recently published the 'Cyber Security (Security Standards for Smart Device) Rules 2025'. These rules require mandatory cyber security in most smart devices (excludes desktop computers, laptops, smartphones and tablet computers) purchased in Australia by consumers. It includes the requirement "Manufacturers publish a means to report security issues – allowing security issues to be reported to the manufacturer, with status updates on the resolution of these issues" and following a 12-month transition period these rules will commence for products manufactured on and from 4th March 2026, "that are intended for personal, domestic or household use". This matches the UK's PSTI regulatory requirements.

10. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/03.01.03_60/en_303645v030103p.pdf
11. https://www.iso.org/standard/72311.html

Europe

The EU Cyber Security Resilience Act (CRA) is expected to supersede the EU Radio Equipment Directive (RED) 2014/53/EU and to avoid the duplication of similar regulations, the RED directive is planned to be repealed on 11th December 2027, the same day the CRA is fully applicable.

EU Regulation 2024/2847, formally adopted on October 23, 2024, and officially titled the Cyber Resilience Act (CRA) is legislation created to drive improvements in the cyber security capabilities of nearly all software or hardware Products with a Digital Element (PDE). Any eligible product sold or distributed in the EU must comply with the requirements of the CRA and carry a CE mark to demonstrate conformity.

Some products such as those in the medical, aviation, automotive and maritime equipment verticals are not included in CRA as they are already covered by other EU regulations and legislation.

Obligations under CRA are different depending on the role of the company i.e. manufacturer, importer or distributor (in the same way as the UK's PSTI Act). Manufacturers of PDEs like the ones covered in this report are expected to carry much of the burden.

Understanding Vulnerability Disclosure in the CRA

It is not easy for the lay person to find the information about what exactly is required from manufacturers under the CRA, beyond the requirements in the Final Text of the Act itself[12]. The technical standards for CRA are still in draft form at the time of this report's publication. This report's publication was deliberately delayed until some clarity was given on the detail of vulnerability disclosure requirements.

The researchers of this report also reached out to various experts, some of whom had contributed to the CRA standardisation process. There was no common view on the expectations and even some confusion caused by the naming, particularly around "disclosure of vulnerabilities", with some mixing it up with mandatory reporting to the EU. This confusion is understandable because the terminology being used is close and overlapping in different areas.

Deadlines have been published for conformance to the CRA's requirements, with complete conformity expected by the end of 2027. Germany's BSI has some useful information on its website[13].The site states that the 11th of September 2026 deadline is: "Obligation to report vulnerabilities and security incidents". However, what this really means is "report actively exploited vulnerabilities to National Authorities' CSIRTs and to ENISA". It immediately creates confusion with vulnerability reporting by security researchers.

One expert stated that this earlier timeline might not be achievable because there are dependencies on other elements being implemented that are only required to be complied with by the end of 2027.

12. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R2847
13. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

CRA Standards for Vulnerability Disclosure

Unfortunately, one of the problems of understanding what is actually required is a lack of transparent, open and free-to-read standards. It took some time to be able to discover the (draft) standards that manufacturers are expected to comply with.

prEN 40000-1-3:2025, Cybersecurity requirements for products with digital elements – Part 1-3: Vulnerability Handling is a draft standard from CEN-CENELEC for CRA. It is available publicly via the Belgian National Standards portal, which was shared by helpful individuals via LinkedIn[14].

The draft standard doesn't appear to have been written with input from security researchers themselves. Rather than distinctly dealing with the issue of vulnerability reporting by security researchers to manufacturers (for which international standards already exist), there has been an attempt to tackle all elements of vulnerability handling in one document. This has led to the unnecessary entanglement with other software supply chain requirements such as for Software Bill of Materials (SBOMs). The work also includes expectations on manufacturers to monitor for vulnerabilities from public and private sources.

The draft standard further creates naming confusion, for example between vulnerability disclosure and vulnerability reporting (without considering the obvious clash with the CRA's final text about reporting to CSIRTs) and the clash in the use of "Reporters" when it comes to security researchers.

There are other problems with the CEN-CENELEC draft specification. Without being a full critique of that document, some examples of issues include:

- The use of 'responsible' when it comes to disclosure practices and security researchers has long been considered to be subjective towards the security researcher as somehow acting irresponsibly when history has proven that it is more often the manufacturer or receiver of vulnerabilities that acts irresponsibly (or fails to act).
- The text is unnecessarily complicated and primarily geared for compliance testing rather than utility.
- The specification gives get-outs for manufacturers, such as allowing the existence of a customer service address as a means for reporting security vulnerabilities (which has historically been disastrous for security researchers). Other requirements such as requiring a coordinator for handling vulnerabilities (an important aspect), are caveated with 'where appropriate' meaning that manufacturers could simply opt not to deem it appropriate to have a coordinator.

14. https://app.nbn.be/data/r/platform/public-portal/pdf-reading-room1?p45_id=3463447&p45_languagecode=en&clear=45&session=61887118899144&cs=1dZnZQwwegsTVrN-0fvH8QaloFkSqwPFBn0Fd-e8LNn6wdZ08-pQpeGKhnN2hevc-wYWSKtcGDjKoqbz230CRrkg

CRA Standards for Vulnerability Disclosure (Cont.)

While the evolution of CVD and reporting practices is to be expected, the first impressions of the draft CEN-CENELEC standard is that it diminishes the role of the security researcher that is reporting the vulnerability, while making it more complicated for manufacturers to deal with such reports. There is a heavy compliance-biased approach to something that should be agile enough to deal with all scenarios.

One of the key problems observed by Copper Horse researchers has been the confusion of nomenclature used both in the CRA's legal text and the draft CEN-CENELEC standard. The term 'vulnerability disclosure' is commonly used in the security research community to mean a hacker or security researcher finding a vulnerability, then disclosing it to a manufacturer, before eventually the issue is made public. This is not about "disclosure of vulnerabilities" to authorities such as the EU. Unfortunately, in the CRA, this is exactly what the text of Annex I states "...disclose fixed vulnerabilities to the European vulnerability database...", further compounding the confusion with "...disclosure of the incidents...".

A more elegant solution to this would be to use the term "share vulnerability information" when it comes to passing on information to the authorities, because by that point, the vulnerability has already been disclosed by the researcher to the manufacturer. In Article 14 – Reporting obligations of manufacturers, clearer text is used, in that it requires manufacturers to report actively exploited vulnerabilities to National Authorities' CSIRTs and to ENISA, the EU's Cybersecurity Agency. These are treated as incidents and the text of the Article does not use the term "disclose".

The reason why these naming issues are important is because many manufacturers do not fully understand the background or even the basics of coordinated vulnerability disclosure. It is recommended that standards bodies attempt to resolve these potential conflicts and that National Authorities and ENISA provide information to help to alleviate this confusion.

Conclusion

This report has continued to expand on the original dataset of 332 manufacturers, increasing to 491 in 2025. This report remains the world's most comprehensive and long-running research tracking the topic of IoT security adoption by manufacturers.

All the data used in this report is available under a Creative Commons 4.0 license, for use by anyone including industry and governments, for transparency or validation purposes, and for further study by researchers interested in the subject of vulnerability disclosure.

The 2025 report has shown a continued trend towards adoption of vulnerability disclosure policies, but not an accelerated trend. This is concerning as it would be reasonable to expect that an acceleration of adoption would happen, with current and imminent legislation and regulation around the world requiring manufacturers to act, particularly in Europe. However, with 2025's figures, the long-term predicted trend of adoption, which indicates when manufacturers might reach 100% compliance has re-aligned itself with this report's previous years' predictions – a full-adoption date of around 2040.

A very positive outcome of 2025's report is that the number of companies passing both parts of the threshold test (meaning they both have a policy and provide information on expected timelines) has increased by nearly a third – an additional 39 vendors to a total of 136. This list includes some very big companies, which also provide a lot of the product volume to the market. It is not possible to measure IoT product factory output or total sales by these companies unfortunately – the report is only able to meaningfully measure the existence of the manufacturers.

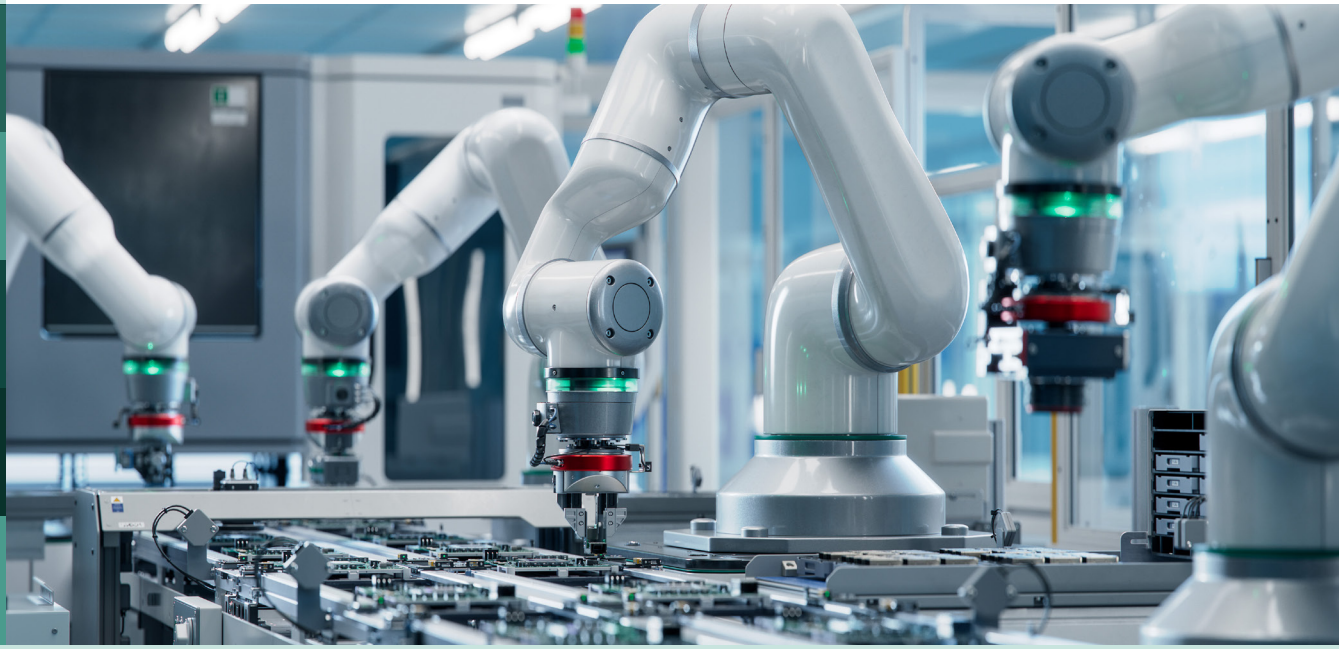
Conclusions (cont.)

Passing the threshold test means that more companies are compliant with the UK's PSTI Act when it comes to vulnerability disclosure and furthermore, they are using more comprehensive policies, making it easier for security researchers to report vulnerabilities.

Ultimately, purchasers of connected consumer products from major retailers are demonstrably being better protected.

The majority of retailers examined for this research now stock products from manufacturers with vulnerability disclosure policies, which is an extremely good marker for increased overall security and can be seen as a positive reflection on both those manufacturers and the retailers themselves, probably synonymous with high-quality digital products. This also indicates that the manufacturers that consumers gravitate towards (generating a high volume of sales) are taking vulnerability disclosure seriously. It means that ultimately, purchasers of connected consumer products from major retailers are demonstrably being better protected.

The remaining manufacturers in the dataset that do not pass the threshold test or do not have policies, represent part of a 'long tail' of potentially insecure consumer IoT that creates cyber security risk for everyone. It remains that over half of the manufacturers in this dataset do not have any method for security researchers to contact them if they discover an issue in a product. This market situation continues to be inadequate, considering that legislation and regulation is in place in some parts of the world and in others is imminent. The EU Cyber Resilience Act will not take full effect until 2027. By this time manufacturers that wish to sell products in the EU will be required by law to have a coordinated vulnerability disclosure policy or face fines or potential removal from the market. It is concerning to see so many manufacturers persist in not adopting what is quite a simple security mechanism to implement. That's just the part that is visible to the public, what about the security of the products themselves? The insecurity canary is singing loud about these manufacturers.



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	FireAngel.	MSI	Sensibo
Amazfit (Zepp Health)	Foscam	Mysa	Shark
Anker, Eufy	Frameo	Nanit	Siemens
Apption Labs	Furbo	NanoLeaf	Signify – Philips Lighting
Aqara	Gardena	Neff	Simpled
Arris (Commscope)	GE Appliances	Netatmo	Smarter Applications
Belkin	Google	Nuki	SonicWall
Best Buy, Insignia	Govee	Omron	Sonoff
BlueAir	Hangzhou XiongMai Technology	OnePlus	Sonos
Bosch	Hanwha, Wisenet	ONKYO	SpaceTalk
BroadLink	HMD Global (Nokia Mobile)	OPPO	Square
Brother Industries, Ltd	HONOR	Oukitel	SUUNTO
BT	Hoover	Owlet	SWANN
Café	HP	Panasonic	SwitchBot
Candy	HTC	Peloton	Synology
Canon	Huawei	PetCube	Tado
Canon, IRIS	Husqvarna	PetLibro	ThermoPro
Casio	IglooHome	Philips	Tile (Life360)
Citizen	Intelbras	Pico	TP-Link
Daikin	iRobot	Procter & Gamble, Oral-B	Tractive
Dell	June	Qardio	Trust
Devialet	Lenovo	Qnap	TVT
Drayton	LG	Reflex Active	Twinkly
Dyson	Logitech	RENPHO	Voxx International, Klipsch
Ecobee	Logitech, Ultimate Ears	Reolink Digital Technology	Weber
Eero	Lorex	Ring	Western Digital
EGLO	Lutron	Roberts Radio	Whirlpool
Einhell	Meross	Roborock	Whisker
Electrolux	Meta	Roku	Wink
Elgato, eve	Microsoft	Samsung (SmartThings)	Withings
Energenie	Midea	Schlage, Allegion	WyzeCam
Eve	Miele	Segway	Xiaomi (MI)
EZVIZ	MOTOROLA	Seiko Epson	X-Sense
FIBARO	Motorola Mobility	Sengled	ZTE

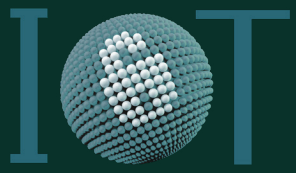
Annex (cont.)

Acer	Devolo	Linksys	SimpliSafe
Amazon	D-Link	Lovense	Skylight
Apple	Draytek	Loxone	Sony
ARLO	Ecovacs	Marshall	Sphero
ASUS	Feit Electric	Nespresso	Starlink
Audio Pro	FitBit	Netgear	SumUp
August	FLiR	NVIDIA	Tapplock
AVM	Garmin	onn	TomTom
Beurer	Hikvision	Oura	Trane
BLINK	Hive	Phyn	Tuya
boAt	Honeywell Home (Resideo)	Polar	Vivo
Bose	JBL	Ray-Ban	Vtech
Buffalo	Kobo	Samsung (Galaxy Watch)	WiZ (Signify)
Dahua	Lexmark	Samsung (Mobile)	Yale
De Longhi	Lifx	Samsung (Smart TV)	ZyXEL
Deutsche Telekom	Lightwave	Sekonda	

360	Baytion	DigitalKeys	Goldair
116 Plus	BeBird	Diyarts	Greater Goods
2NLF	Beeline	Doogee	Grohe
ABIR	Behmor	Double Robotics	Groove
ACEMAX	BELLABEAT	Dreame	Guardian Technologies (Lasko)
ACTi	Blackview	Dreo	Hama
AdhereTech	BLU Products	Edimax	Hank
ADT	BPT	ELAiCE	Hatch
AEG	BTICINO	Elecom	Hatch Baby
Aeon Labs, Aeotec	Calex	Eminent	HAVIT
AIGOSTAR	Canary	EMOOR	Haylou
Airboxlab	Catapult Sports	Enabot	HeimVision
Aiwa	Chamberlain	Epikasa	Hidrate
AliveCor	Chamberlain	eq-3	Hikers
Anmossi	Circle	Estimote	Hoco
Anoto	Click and Grow	Etekcity	Hombli
Anova	COA	First alert	HTN
Anran	Comap	Flux Smart	Hunterfan
ANTELA	Copeland (Emerson)	FREDI	Hyrican
ApnaCam	Cosori	Garadget	i2GO
Aranet	CP Plus	GARETT	iFAVINE
Arugo	CTRZQ	Garza	IFITech
ASAKUKI	Cube	Gavdhe	iHealth
Aubess	Curb (Powered By Elevation)	GBC	iHuniu
Aura	Current Labs	Geekee	ilumi
Avidsen	Daybetter	Geeni	InBody
Awair	DCU	GENERIC	Infinix
B&O	Deeper	Genius Hub	INLINE
B.K. Licht	DENON	GHome Smart (Gosund)	Innr
Bangtan	DEWENWILS	GNCC	Insteon

Annex (cont.)

InteraXon Inc
Iris Ohyama
iTime Jr.
Jasco
Jura
JWCOM
Kangaroo
Kashimura
Keen Home
KESHUYOU
KeySmart
Kidde
KIQULOV
Klarstein
Kolibree, Baracoda
Kolke
Konnek Stein
Koogeek
Krups
Ksipze
Ktaxon
Kwikset
Lampaous, LUMENMAX
Laresar
Laurastar
LAXASFIT
Lenbrook Industries, Bluesound
Leotec
LetsFit
Level
LifeFitness
LIGE
Lithe
Lockin
Lockly
Lohas
lulshou
Maizic
Matrix
Mattel, Fisher-Price
Maxevis
MBG LINE
MEGABRIGHT
Merkury Innovations
MIPOW
Moen
Moes House
MoKo
Moleskine
Muvit
MySpool
NAIM
Nautica
Neo
Neurio, Generac
Neutron
NEXXT SOLUTIONS
NGTeco
Night Owl
Nivian
NO NAME
NO NAME 2
Noise
NordicTrack
Novostella, Ustellar
Osram
Otio
Overmax
Oyajia
PandaX
Perfect Company
Pixbee
Plus Style (+Style)
PNI
Popglory
Positivo
Proform (ICON fitness)
Promate
Qiwa
Qrio
Rachio
RADEMACHER
Radley
Ratoc Systems
Razuvious
REHENTINT
Remotec
repetsun
Revolo
Rojeco
Roost
Ruark
Ruveno
Seneye
Sensoria
Servo
Shenzhen Neo
shine-tale
SKY HUB
Skybell
Sky-Touch
Sleep Number
Small
Smartbell
SmartyPans
SMD Technologies branded as Connex Connect
SNARIYOVSN
SOSAFE
SSC-LUXon
SWAN
Tanita
TCL Corporation (Alcatel)
Teckin
Teckin
Teclast
Tefal
TEKXDD
Theatro
Therabody
TIBO
Tichondrius
Tomshine
Topesel
TopVision
Tracking Point
Trade Shop Italia
TRENDnet
TVLIVE
TytoCare
Tzumi
UanTii
UBTECH
Ultenic
Ustellar
V380
Valdus
ValueLights
Vankyo
Vaultek
Vava
Veho
Veho-lifestyle
Velco
Vemer
Vine
Vitamix
Vivint
Vivitar
Volibel
Wattbike
Wattcost
Wearable X
WeeKett
Weenect
Weight Gurus (Greater Goods)
We-Vibe
Whistle
Wimius
Winix America
Wsdcam
X Rocker
X10
XCOAST
XODO (Contixo)
Xoopar
Xperi, DTS
Yamaha Pro Audio, Yamaha Corporation
Yeelight
YP
Yunmai
Zeeq
Zmodo Technology



www.iotsecurityfoundation.org

www.copperhorse.co.uk

59-60 Thames street, Windsor, Berkshire, UK, SL4 1TX
+44 (0) 208 1337733 @copperhorseuk