cetome

we make cyber work

IoT Security

VDP Accessibility and Usability in Consumer IoT

Author: C. LEVY-BENCHETON

Date: 1/02/2024

Table of Contents

Introduction

The Internet of Things ("IoT") is an ecosystem where connected devices interact with other devices and services. In this ecosystem, IoT products combine hardware, software and network capabilities to collect data, analyse them and perform tasks.

This creates a large attack surface, with vulnerabilities causing risks to systems, data, and users (privacy, safety). Due to the large number of IoT systems in the world, a vulnerability in one product can affect millions of systems at the same time. And because of their nature, most IoT products are an easy target for attackers.

To limit the impact of insecure IoT on our society, multiple cyber security regulations are now in place. These regulations require IoT manufacturers to manage cyber risks during the product development phase and after product release. Manufacturers must keep track of vulnerabilities, assess their risks on products, users and data, and fix them (usually with a patch).

For that purpose, most regulations require IoT manufacturers to implement a public Vulnerability Disclosure Policy ("VDP") to receive vulnerability reports from external stakeholders. To do so, manufacturers can follow international standards such as ETSI EN 303 645 (provision 5.2-1), ETSI TR 103 838 or ISO 29147.

A public VDP is a good tool to improve product security. This is also a requirement of most IoT cyber security regulations. However, VDP adoption in consumer IoT is still limited as shown by the IoT Security Foundation and CopperHorse Ltd in their yearly reports.

We decided to explore the accessibility and usability of VDP in consumer IoT, a regulatory requirement for IoT manufacturers. Making VDP accessible and usable is not only a compliance requirement, it is necessary to encourage the submission of vulnerability reports.

We discovered that many public VDP have issues regarding accessibility or usability. We also found that international cyber security standards do not include any accessibility requirements.

In this study, we evaluate the accessibility and usability of VDP in consumer IoT by looking at several metrics. We highlight various issues that limit the effectiveness of VDP and that could cause issues to manufacturers with their regulatory compliance. Finally, we propose a list of recommendations to make IoT VDP more accessible. This will improve product security and help manufacturers comply with their regulatory requirements more easily.

Scope and Methodology

Scope

The scope of this study focuses on the accessibility of the vulnerability disclosure policy and its usability in various consumer IoT products. The list of products was chosen randomly among renowned brands, products we own, products we want to buy, products with a cyber security label and some of their competitors.

We consider all variants of the VDP such as coordinated disclosure, responsible disclosure, etc.

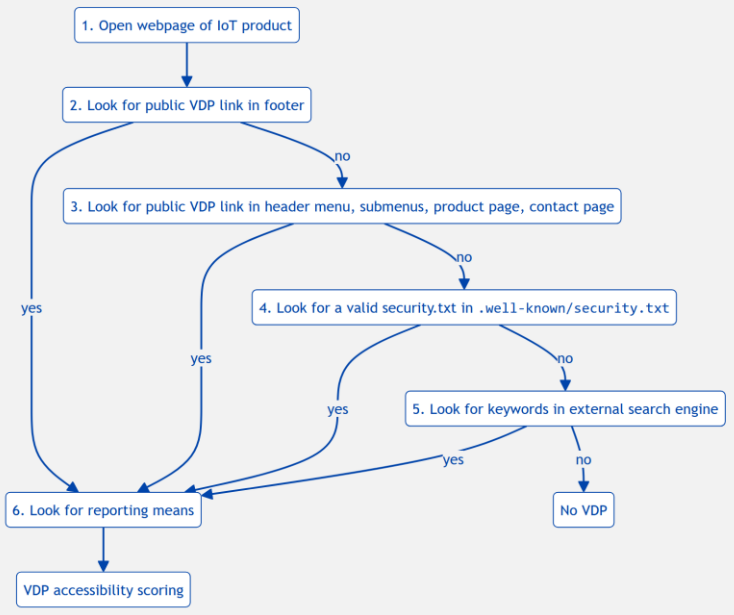
Sectors outside IoT products are out of scope even though the results and our recommendations are directly applicable to any domain (IT, Cloud, infrastructure, OT, etc.).

Accessing public VDP

We tried accessing existing public VDP as follows:

1. Open webpage of IoT product or its manufacturer
2. Look for public VDP link in footer
3. Look for public VDP link in header menu, submenus, in the product page, in the contact page
4. Look for a valid security.txt in **.well-known/security.txt**
5. Look for keywords in an external search engine
6. Look for reporting means (webform, email address)
7. Evaluate VDP accessibility scoring

Our methodology for accessing a public VDP


1. Open webpage of IoT product
2. Look for public VDP link in footer
no
yes
3. Look for public VDP link in header menu, submenus, product page, contact page
no
yes
4. Look for a valid security.txt in .well-known/security.txt
no
yes
5. Look for keywords in external search engine
yes
no
6. Look for reporting means
No VDP
VDP accessibility scoring

We mainly relied on manual navigation to discover the public VDP webpage. When we struggled to find a link, we searched for keywords such as:

- vulnerability
- disclos* *(disclose, disclosure)*
- report
- security
- PSIRT
- CSIRT
- trust

VDP accessibility scoring

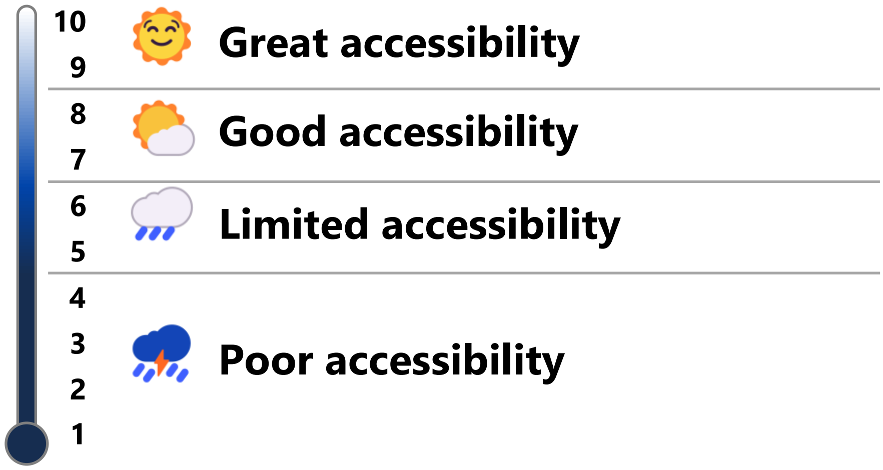
We looked at the following metrics to score the accessibility of public VDP. The VDP accessibility scoring depends on the sum of these metrics (over 10 points).

The following table details the different metrics.

Metrics	Parameters	Score
Accessibility of the VDP from the frontpage	Link in the footer menu	3
	Link in a header sub-menu	2
	Link in another part of the website	1
	VDP not accessible directly, it requires an external search engine	0
Number of clicks to access the VDP from the frontpage	1 or 2 clicks	3
	3 or 4 clicks	2
	5 clicks or more	1
	VDP not found using navigation	0
Number of clicks to submit the report from the public VDP webpage	1 click	3
	2 clicks	2
	3 clicks or more	1
Bonus point: **presence of a valid security.txt**	Security.txt is compliant with RFC 9116	+1

The VDP accessibility score is either “great”, “good”, “limited” or “poor” according to the sum of all metrics:

VDP accessibility score



Evaluate your VDP Accessibility Score

VDP ACCESSIBILITY IN STANDARDS AND REGULATIONS

We looked at VDP accessibility requirements in IoT cyber security standards and regulations. Only 2 regulations require making the VDP accessible: the EU Cyber Resilience Act and the UK PSTI (with implicit requirements that could be interpreted as mandatory).

ETSI EN 303 645

The first international standard to establish a cyber security baseline for consumer IoT requires a VDP with a minimum level of information (provision 5-2.1). However, it has no requirement to make this VDP accessible.

NIST IR 8259B

NIST mandates non-technical requirements supporting their core baseline for IoT cyber security. They establish requirements for "documentation" including the publication of a VDP with a point of contact. However, there is no mention of making the VDP accessible either.

Regulatory requirements in the United Kingdom

In the UK, the PSTI Regulations 2023 requires manufacturers (and distributors) of consumer IoT to make a point of contact accessible to report vulnerabilities in Schedule 2, Art. 2(3).

These accessibility requirements only concern the point of contact but they should easily apply to the VDP itself.

> **Schedule 2, Art. 2(3) of the UK PSTI Regulations**
> Information on how to report security issues
>
> (3) The information in sub-paragraph (2) must be accessible, clear and transparent, and must be made available to [a person] P—
>
> (a) without prior request for such information being made;
>
> (b) in English;
>
> (c) free of charge; and
>
> (d) without requesting the provision of P's personal information.

Regulatory requirements in the European Union

The Radio Equipment Directive Delegated Act ("RED DA") for Cyber Security is a technical regulation and it does not require a vulnerability disclosure policy.

The Cyber Resilience Act is an upcoming regulation for products with digital elements. Article 10(10) in the final text requires IoT manufacturers to make accessible their requirements in Annex II which include a VDP.

> **Annex II of the EU Cyber Resilience Act**
> Information and instruction to the user
>
> 2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found

VDP ACCESSIBILITY ISSUES

We discovered several issues that make reporting vulnerabilities difficult. These issues appear at multiple IoT manufacturers, no matter their sector, their size or their geography. Moreover, some of these issues may lead to early disclosure, affecting the security of IoT products, customers and users, as well as the reputation of their manufacturer.

With this study, we encourage all consumer IoT manufacturers to review the accessibility and usability of their VDP in the light of these different issues. We released a free tool to evaluate your VDP accessibility score.

Evaluate your VDP Accessibility Score

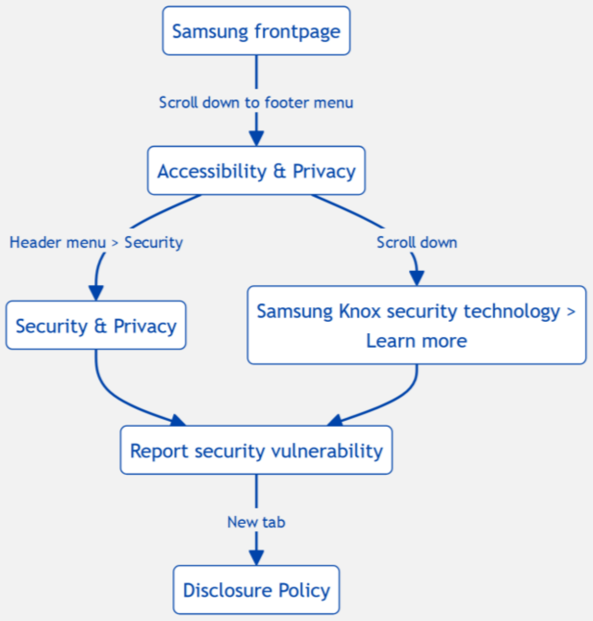
Issue 1. VDP is not directly accessible

When the VDP exists, it should be accessible easily, either from the product website or from the manufacturer's corporate website. Sometimes this VDP is not directly accessible because it takes too many clicks to access it or there is no direct link to it.

It is also possible to access this VDP by using a search engine. However, this is not optimal and vulnerability reporters may lose patience, going to social media to find a point of contact or by making their findings public immediately. This could create reputational risks and other internal troubles for IoT manufacturers.

The easiest solution is to make the VDP directly accessible on the product website.

User journey for accessing Samsung VDP



Issue 2. Inconsistent accessibility across products or markets

We explored how IoT manufacturers implement their VDP across different markets and / or across different brands and subsidiaries. We discovered several interesting issues:

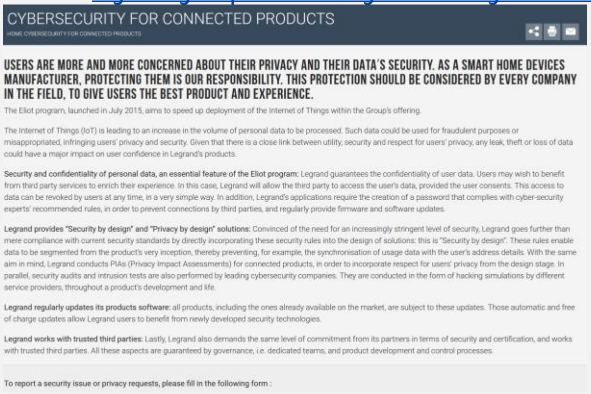
- **Multiple VDPs for different products or brands.** This can lead to a misalignment in scope or treatment of reports, especially when these products or brands share the same resources (development team, source code, user account, backend services).
- **No VDP for some products or brands**. This could rapidly become confusing when other products or brands have a VDP.

- **Different reporting requirements for different markets**. This denotes a compliance-driven approach which is not helpful for security.
- **No VDP for similar products on different markets**. This is not acceptable: the same products should have similar requirements across all markets.

We can imagine that these issues are related to the internal organisation of big corporations. However, we believe they could benefit from simplifying their product security with one single VDP for all markets, all products and all brands. This will make things more efficient and easier to manage.

Legrand and its brand Netatmo have different reporting requirements

Legrand has a very detailed policy on the corporate website with a reporting webform
Source: legrandgroup.com/en/cybersecurity-connected-products



CYBERSECURITY FOR CONNECTED PRODUCTS

HOME CYBERSECURITY FOR CONNECTED PRODUCTS

USERS ARE MORE AND MORE CONCERNED ABOUT THEIR PRIVACY AND THEIR DATA'S SECURITY. AS A SMART HOME DEVICES MANUFACTURER, PROTECTING THEM IS OUR RESPONSIBILITY. THIS PROTECTION SHOULD BE CONSIDERED BY EVERY COMPANY IN THE FIELD, TO GIVE USERS THE BEST PRODUCT AND EXPERIENCE.

The Eliot program, launched in July 2015, aims to speed up deployment of the Internet of Things within the Group's offering.

The Internet of Things (IoT) is leading to an increase in the volume of personal data to be processed. Such data could be used for fraudulent purposes or misappropriated, infringing users' privacy and security. Given that there is a close link between utility, security and respect for users' privacy, any leak, theft or loss of data could have a major impact on user confidence in Legrand's products.

Security and confidentiality of personal data, an essential feature of the Eliot program: Legrand guarantees the confidentiality of user data. Users may wish to benefit from third party services to enrich their experience. In this case, Legrand will allow the third party to access the user's data, provided the user consents. This access to data can be revoked by users at any time, in a very simple way. In addition, Legrand's applications require the creation of a password that complies with cyber-security experts' recommended rules, in order to prevent connections by third parties, and regularly provide firmware and software updates.

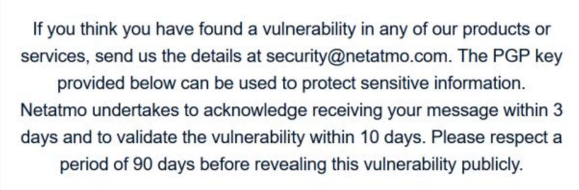
Legrand provides "Security by design" and "Privacy by design" solutions: Convinced of the need for an increasingly stringent level of security, Legrand goes further than mere compliance with current security standards by directly incorporating these security rules into the design of solutions: this is "Security by design". These rules enable data to be segmented from the product's very inception, thereby preventing, for example, the synchronisation of usage data with the user's address details. With the same aim in mind, Legrand conducts PIAs (Privacy Impact Assessments) for connected products, in order to incorporate respect for users' privacy from the design stage. In parallel, security audits and intrusion tests are also performed by leading cybersecurity companies. They are conducted in the form of hacking simulations by different service providers, throughout a product's development and life.

Legrand regularly updates its products software: all products, including the ones already available on the market, are subject to these updates. Those automatic and free of charge updates allow Legrand users to benefit from newly developed security technologies.

Legrand works with trusted third parties: Lastly, Legrand also demands the same level of commitment from its partners in terms of security and certification, and works with trusted third parties. All these aspects are guaranteed by governance, i.e. dedicated teams, and product development and control processes.

To report a security issue or privacy requests, please fill in the following form :

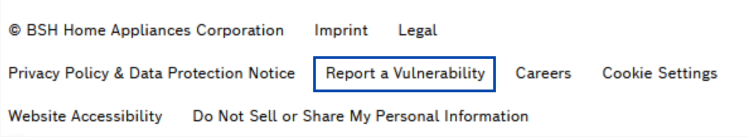
Netatmo policy is less verbose and reporting uses an email with PGP
Source: netatmo.com/security-incidents



If you think you have found a vulnerability in any of our products or services, send us the details at security@netatmo.com. The PGP key provided below can be used to protect sensitive information. Netatmo undertakes to acknowledge receiving your message within 3 days and to validate the vulnerability within 10 days. Please respect a period of 90 days before revealing this vulnerability publicly.

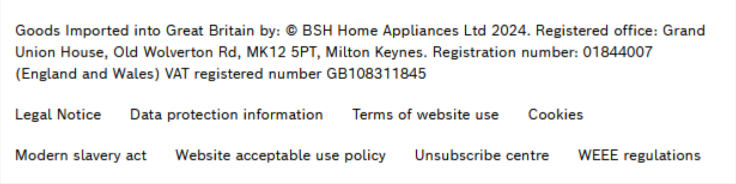
Bosch Home has a link to the VDP in the footer menu on the US website but not on other markets

"Report a vulnerability" in the footer menu in the US website
Source: bosch-home.com/us/



© BSH Home Appliances Corporation   Imprint   Legal
Privacy Policy & Data Protection Notice   Report a Vulnerability   Careers   Cookie Settings
Website Accessibility   Do Not Sell or Share My Personal Information

No link to report a vulnerability in the UK website
Source: bosch-home.com/uk/



Goods Imported into Great Britain by: © BSH Home Appliances Ltd 2024. Registered office: Grand Union House, Old Wolverton Rd, MK12 5PT, Milton Keynes. Registration number: 01844007 (England and Wales) VAT registered number GB108311845

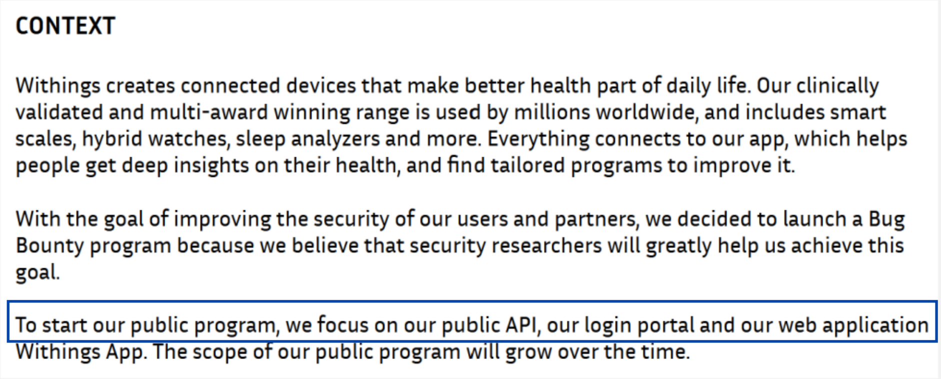
Legal Notice   Data protection information   Terms of website use   Cookies
Modern slavery act   Website acceptable use policy   Unsubscribe centre   WEEE regulations

Issue 3. Public VDP does not cover products

Some manufacturers of consumer IoT have a public VDP that does not cover their products. Their existing VDP would only cover public websites and potentially Cloud APIs.

This could quickly become an issue if product vulnerabilities are not reported or worse, if valid reports are deemed "out of scope" and simply ignored. In this case, reporters could decide to make their findings public to avoid unnecessary effort with the manufacturer.

Withings VDP uses a public bug bounty platform but it does not integrate devices
Source: yeswehack.com/programs/withings-public-program



CONTEXT

Withings creates connected devices that make better health part of daily life. Our clinically validated and multi-award winning range is used by millions worldwide, and includes smart scales, hybrid watches, sleep analyzers and more. Everything connects to our app, which helps people get deep insights on their health, and find tailored programs to improve it.

With the goal of improving the security of our users and partners, we decided to launch a Bug Bounty program because we believe that security researchers will greatly help us achieve this goal.

To start our public program, we focus on our public API, our login portal and our web application Withings App. The scope of our public program will grow over the time.

Issue 4. Invalid security.txt

The security.txt is currently not a requirement in IoT cyber security standards. Yet, it is a great way to make a VDP more accessible:

- It is always located at the same URL (/.well-known/security.txt).
- It must point to the policy webpage and should communicate a single point of contact.
- It is a simple text file that only requires little maintenance.

However, many IoT manufacturers with an accessible VDP do not have an associated security.txt. And when they do, it is possible that their security.txt is invalid:

- **The security.txt expiration date is in the past**. This is the most common issue as setting up a security.txt is usually done once and content update is often overlooked. However, this is not really an issue in real-life if the URLs are still accessible.
- **The security.txt is incomplete** and does not contain all mandatory fields (a link to the VDP and the expiration date).
- **Wrong content in the security.txt**. In most cases, the security.txt contains one or more stale links. In one instance, we discovered an invalid security.txt pointing to the VDP of the CRM vendor.

Airthings has an invalid security.txt pointing to their CRM vendor.
Source: airthings.com/.well-known/security.txt

```
Contact: mailto:security@airthings.com

Policy: https://magento.com/security

Preferred-Languages: en
```

Issue 5. VDP accessible in an unusual way

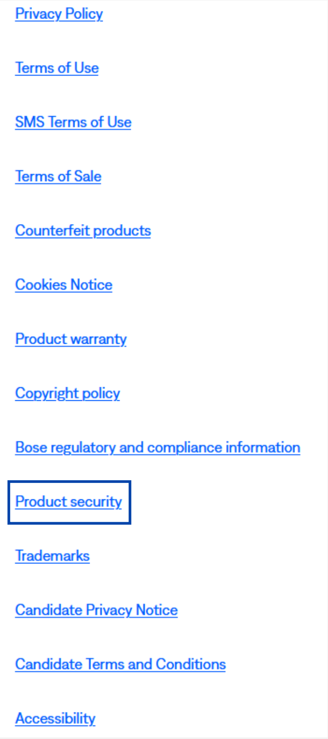
Ideally, product websites contain a self-explanatory link pointing to the VDP. Reporters can find this link on the frontpage (in the footer menu or in the header menu), in a contact page, or in a thematic webpage.

We discovered that some manufacturers place their VDP in very unusual locations that make it very difficult to access, negating any benefits:

- **The VDP is accessible through the privacy notice webpage**. This link to the "privacy notice" is usually found in the footer menu. However, it is an unexpected location for product VDP. Indeed, consumer IoT vulnerabilities go way beyond personal data.
- **The VDP is located under the "legal / compliance" webpage**. This is an unusual location, as it is generally a place for displaying corporate policies (supply chain, sustainability, etc.), not product ones.
- **VDP is hidden in a blog post, in a support page or in a community forum post**. This is not acceptable as nobody would actively search the VDP in these locations (sure, we did but only because we are doing this study).

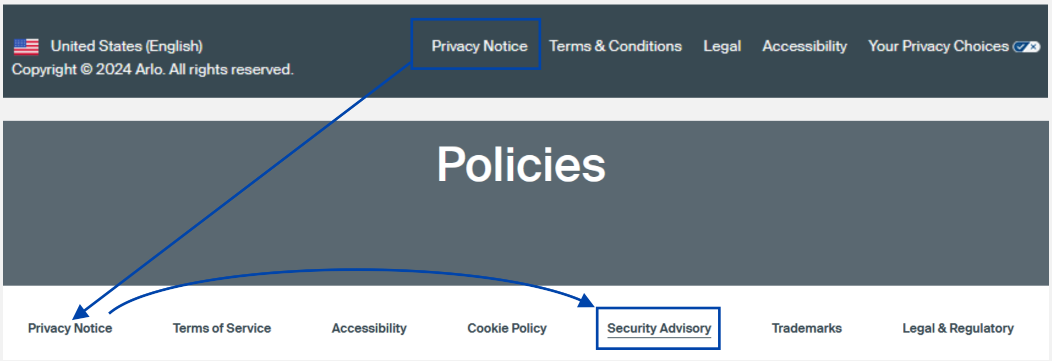
We believe that these manufacturers follow a compliance-driven approach to security. We can only imagine that they follow the same approach for their product development, which is not optimal (to stay polite). We encourage them to improve the accessibility of their VDP by following our recommendations.

Bose VDP is accessible from the Legal link in the footer menu
Source: bose.com/legal/product-security

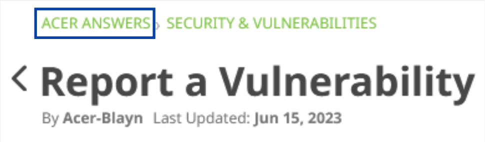


Privacy Policy
Terms of Use
SMS Terms of Use
Terms of Sale
Counterfeit products
Cookies Notice
Product warranty
Copyright policy
Bose regulatory and compliance information
Product security
Trademarks
Candidate Privacy Notice
Candidate Terms and Conditions
Accessibility

Arlo VDP is only accessible after clicking on the "Privacy" link in the footer menu
Source: arlo.com/en-us/security-advisory.html



Acer VDP is accessible after going through the FAQ
Source: https://community.acer.com/en/kb/articles/13285-report-a-vulnerability


ACER ANSWERS › SECURITY & VULNERABILITIES

Report a Vulnerability

By Acer-Blayn Last Updated: Jun 15, 2023

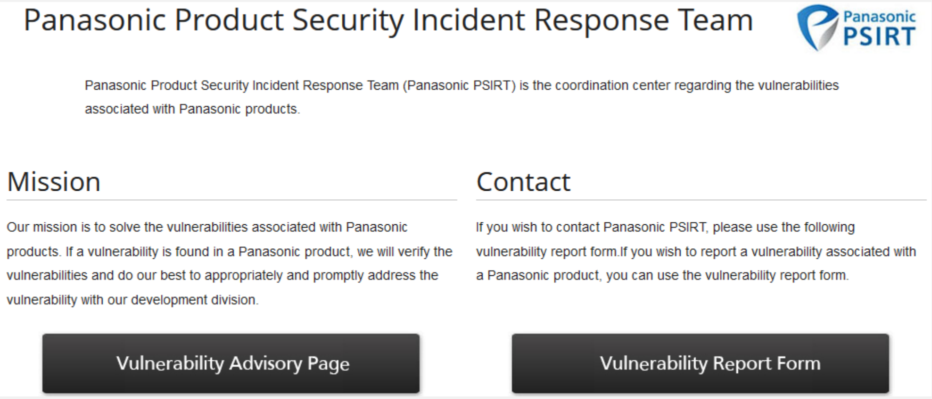
Issue 6. Dedicated product security website not directly accessible

Some IoT manufacturers have a dedicated product security website containing their VDP. This is usually the website of the Product Security Incident Response Team (PSIRT) which is responsible for keeping products secure after release. These websites are usually hosted on their own domain or on a subdomain of the corporate website.

And yet, in several instance it is impossible to reach the dedicated product security website from the product/manufacturer website. It is only possible to discover their existence using an external search engine.

These manufacturers have a very mature security posture in the IoT ecosystem. They should lead by example and make their dedicated product security website more accessible.

Panasonic PSIRT website can only be discovered with a search engine
Source: holdings.panasonic/global/corporate/product-security.html


Panasonic Product Security Incident Response Team

Panasonic PSIRT

Panasonic Product Security Incident Response Team (Panasonic PSIRT) is the coordination center regarding the vulnerabilities associated with Panasonic products.

Mission

Our mission is to solve the vulnerabilities associated with Panasonic products. If a vulnerability is found in a Panasonic product, we will verify the vulnerabilities and do our best to appropriately and promptly address the vulnerability with our development division.

Contact

If you wish to contact Panasonic PSIRT, please use the following vulnerability report form.If you wish to report a vulnerability associated with a Panasonic product, you can use the vulnerability report form.

Issue 7. Vulnerability reporting is private

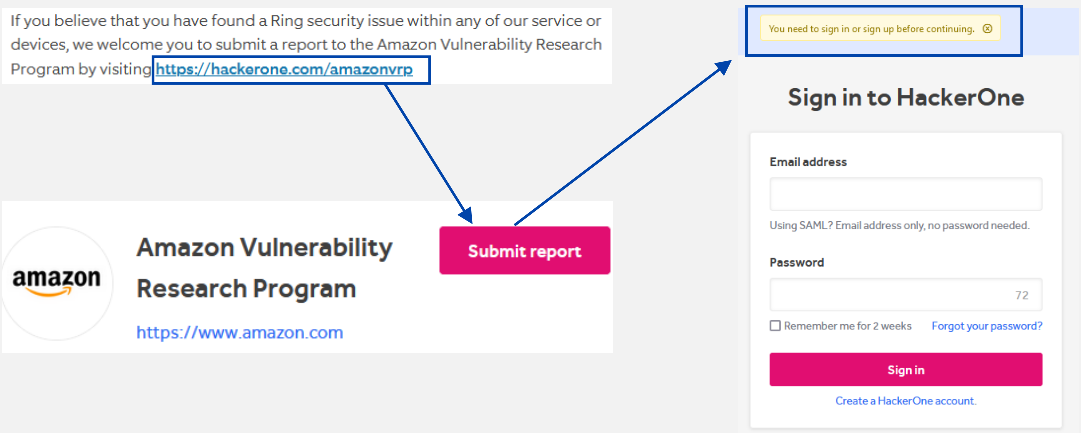
To comply with regulations, vulnerability reporting must be accessible publicly. This means that the point of contact to submit a report must be open, without a user account.

We discovered issues that go against these regulatory requirements:

- Several manufacturers require a login to submit vulnerability reports using an external platform. This means that security researchers must create an account on a third-party service and accept the associated terms and conditions (which can be unfair to reporters). Note that it is perfectly acceptable to use an external platform for VDP reporting as it can be difficult to implement all requirements internally due to the lack of processes, resources or skills.
- Manufacturers with their own VDP reporting capabilities require a user account to submit security issues. Even though it may be a requirement for their bug bounty, public VDP reporting must remain public as security issues affect products on the market.

These IoT manufacturers must understand that their point of contact must be accessible easily as required by IoT cyber security regulations. If they do not align with this requirement, they may be facing important penalties in the coming months.

Ring requires a login to report issues via Amazon dedicated page (hosted on HackerOne)
Source: ring.com/security

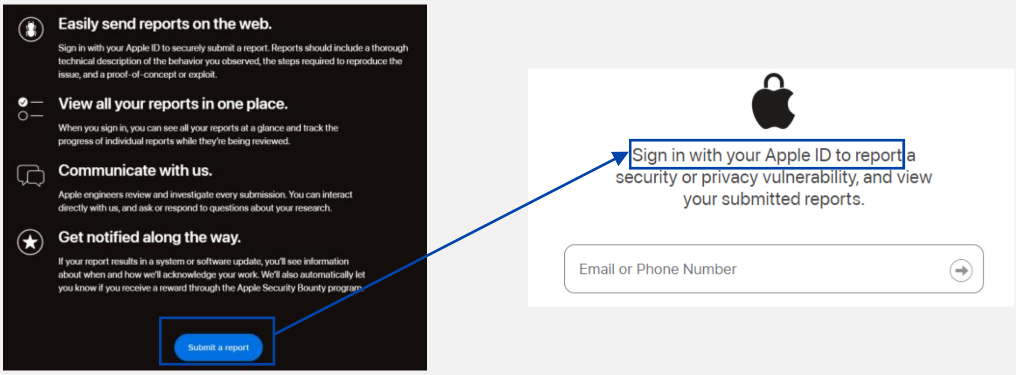


If you believe that you have found a Ring security issue within any of our service or devices, we welcome you to submit a report to the Amazon Vulnerability Research Program by visiting https://hackerone.com/amazonvrp

You need to sign in or sign up before continuing.

amazon
Amazon Vulnerability Research Program
https://www.amazon.com
Submit report
Sign in to HackerOne
Email address
Using SAML? Email address only, no password needed.
Password
72
□ Remember me for 2 weeks
Forgot your password?
Sign in
Create a HackerOne account.

Apple requires a user account to submit a vulnerability report
Source: security.apple.com/bounty/



Easily send reports on the web.

Sign in with your Apple ID to securely submit a report. Reports should include a thorough technical description of the behavior you observed, the steps required to reproduce the issue, and a proof-of-concept or exploit.

View all your reports in one place.

When you sign in, you can see all your reports at a glance and track the progress of individual reports while they're being reviewed.

Communicate with us.

Apple engineers review and investigate every submission. You can interact directly with us, and ask or respond to questions about your research.

Get notified along the way.

If your report results in a system or software update, you'll see information about when and how we'll acknowledge your work. We'll also automatically let you know if you receive a reward through the Apple Security Bounty program.

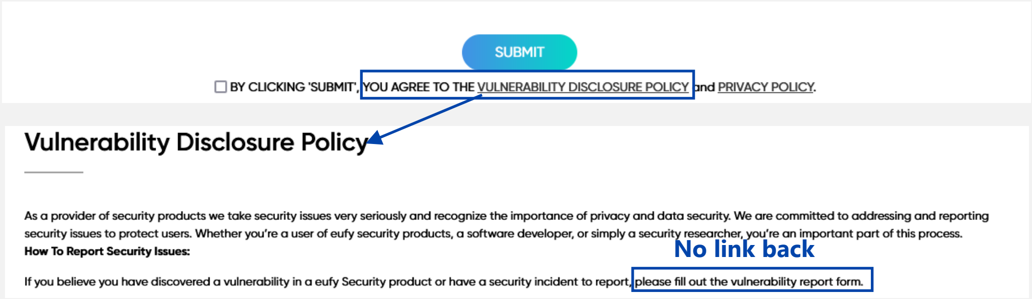
Sign in with your Apple ID to report a security or privacy vulnerability, and view your submitted reports.

Issue 8. Usability issues in VDP webpage

When the VDP reporting page is easily accessible, it is possible that user experience creates issues to reporters. We discovered some usability issues that are easy to fix:

- A reporting webform opening a new link to the VDP. When clicking on this link, a new page opens in the same browser tab. This webpage has no link to go back to the webform. The only solution is to use the "Previous" button on the browser.
- The impossibility to report a vulnerability on all browsers. On one occasion, a manufacturer uses a text box with a button to access their VDP. This button becomes hidden on mobile due to overflow. On another occasion, only Chrome-based browsers display the relevant reporting procedure
- An unnecessary complicated workflow to submit a report. This can discourage most reporters.

Eufy VDP is accessible from the reporting webform but there is no link to go back
Source: us.eufy.com/pages/vulnerability-form



□ BY CLICKING 'SUBMIT', YOU AGREE TO THE VULNERABILITY DISCLOSURE POLICY and PRIVACY POLICY.

Vulnerability Disclosure Policy

As a provider of security products we take security issues very seriously and recognize the importance of privacy and data security. We are committed to addressing and reporting security issues to protect users. Whether you're a user of eufy security products, a software developer, or simply a security researcher, you're an important part of this process.

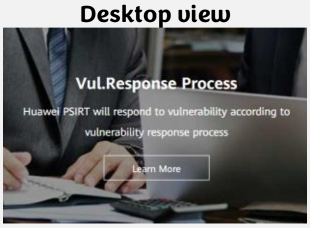
How To Report Security Issues:

If you believe you have discovered a vulnerability in a eufy Security product or have a security incident to report, please fill out the vulnerability report form.

No link back

Huawei VDP is not accessible on mobile. The "Learn More" button disappears the due to overflow
Source: huawei.com/en/psirt

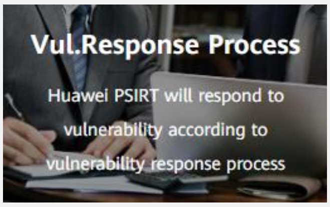
Desktop view



Vul.Response Process

Huawei PSIRT will respond to vulnerability according to vulnerability response process

Mobile view

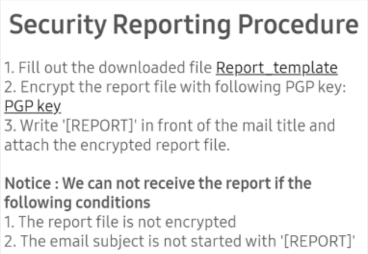


Vul.Response Process

Huawei PSIRT will respond to vulnerability according to vulnerability response process

Samsung reporting is unnecessary complicated and is broken on Firefox
Source: security.samsungda.com/securityReporting.html

Chrome-based browser

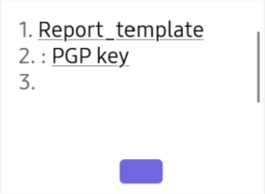


Security Reporting Procedure

1. Fill out the downloaded file Report_template
2. Encrypt the report file with following PGP key: PGP key
3. Write '[REPORT]' in front of the mail title and attach the encrypted report file.

Notice : We can not receive the report if the following conditions
1. The report file is not encrypted
2. The email subject is not started with '[REPORT]'

Firefox



1. Report_template
2. : PGP key
3.

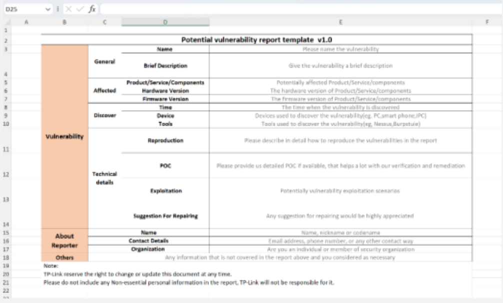
Issue 9. Poor usability of reporting template

A VDP defines the rules for reporting vulnerabilities. When the VDP mandates a reporting template, reports must contain specific information. In turn, manufacturers who receive standardised reports can better identify issues and fix root causes.

The VDP usually communicates this reporting template with an outline or with specific fields in a webform. We discovered that some manufacturers require reporters to submit a binary file. We believe this causes some issues:

- Reporters will have to download a binary file, install the appropriate editing tool and send their final report. This is cumbersome and some reporters may decide to use their own template, or not to disclose at all.
- Binary file formats like .docx or .pdf could potentially leak metadata when the reporter wishes to remain anonymous. This can cause issues in geographies that do not protect vulnerability reporters from legal repercussions.
- A reporting template using a spreadsheet (usually an Excel file) will limit the number of characters per cell. This may require some editing (new lines, new cells) that may break any automation in place on the receiving side.
- Binary file formats could be used for introducing malware at reporters and at manufacturers. This requires additional security requirements.

TP-Link reporting template is an Excel spreadsheet with a character limit per cell
Source: tp-link.com/us/press/security-advisory/

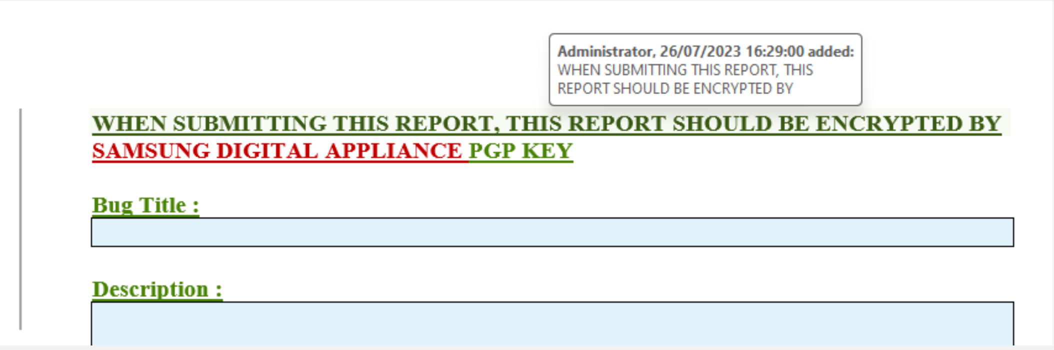


D25

Potential vulnerability report template v1.0			
Vulnerability	General	Name	Please name the vulnerability
		Brief Description	Give the vulnerability a brief description
	Affected	Product/Service/Components	Potentially affected Product/Service/components
		Hardware Version	The hardware version of Product/Service/components
		Firmware Version	The firmware version of Product/Service/components
	Discover	Time	The time when the vulnerability is discovered
		Device	Devices used to discover the vulnerability(eg. PC,smart phone,IPC)
		Tools	Tools used to discover the vulnerability(eg, Nessus,Burpstuie)
	Technical details	Reproduction	Please describe in detail how to reproduce the vulnerabilities in the report
		POC	Please provide us detailed POC if available, that helps a lot with our verification and remediation
		Exploitation	Potentially vulnerability exploitation scenarios
		Suggestion For Repairing	Any suggestion for repairing would be highly appreciated
About Reporter	Name		Name, nickname or codename
	Contact Details		Email address, phone number, or any other contact way
	Organization		Are you an individual or member of security organization
Others	Any information that is not covered in the report above and you considered as necessary		

Note:
TP-Link reserve the right to change or update this document at any time.
Please do not include any Non-essential personal information in the report, TP-Link will not be responsible for it.

Samsung reporting template shows is leaking internal data due to track changes enabled. This could cause further security risks since the editor is "Administrator"
Source: security.samsungda.com/securityReporting.html



Administrator, 26/07/2023 16:29:00 added:
WHEN SUBMITTING THIS REPORT, THIS REPORT SHOULD BE ENCRYPTED BY

WHEN SUBMITTING THIS REPORT, THIS REPORT SHOULD BE ENCRYPTED BY SAMSUNG DIGITAL APPLIANCE PGP KEY

Bug Title :

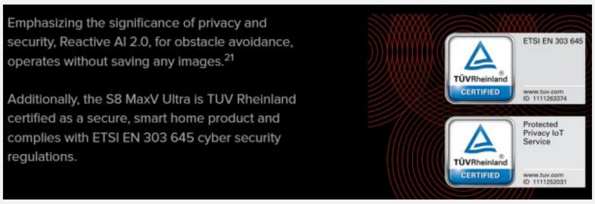
Description :

Issue 10. Products compliant with EN 303 645 with no VDP

In this study, we looked at several products that advertise their compliance with ETSI EN 303 645. They usually display a label issued by a governmental agency or by a private test lab.

As a reminder, a VDP with a single point of contact and clear reporting timelines is a mandatory requirement in EN 303 645 (provision 5.2-1).

Roborock latest vacuum cleaner displays a label "compliant with ETSI EN 303 645"
Source: Roborock S8 MaxV Ultra



Emphasizing the significance of privacy and security, Reactive AI 2.0, for obstacle avoidance, operates without saving any images.[21]

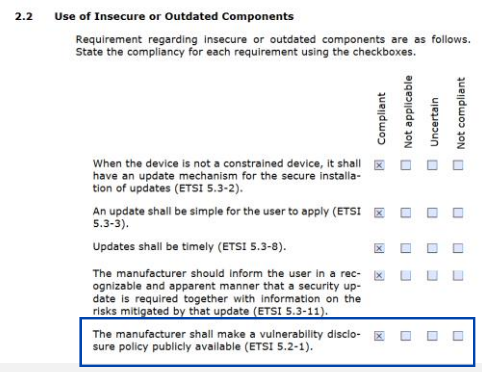
Additionally, the S8 MaxV Ultra is TUV Rheinland certified as a secure, smart home product and complies with ETSI EN 303 645 cyber security regulations.

We found an issue with a government-issued label based on EN 303 645: Tietoturvamerkki. We could not find any VDP for labelled product made by Finnish manufacturers, despite manufacturers reporting their compliance. These manufacturers only have a point of contact. This raises several questions on the credibility of such labels.

For example, Polar declared a publicly available VDP to Traficom, who oversees the label. They only have an email address in a hidden support page, with no timeline (even though it is a requirement of EN 303 645). We contacted Polar and Traficom the 16th of November 2023 with our enquiry. We are still waiting for an answer.

Issues with EN 303 645 compliance issues by the Finnish label (Tietoturvamerkki)

Polar Statement of Compliance
Source: Statement of Compliance (PDF)

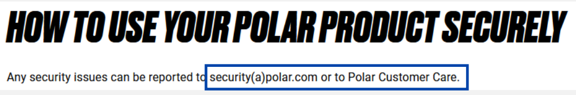


2.2 **Use of Insecure or Outdated Components**

Requirement regarding insecure or outdated components are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compliant
When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2).	☒	☐	☐	☐
An update shall be simple for the user to apply (ETSI 5.3-3).	☒	☐	☐	☐
Updates shall be timely (ETSI 5.3-8).	☒	☐	☐	☐
The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update (ETSI 5.3-11).	☒	☐	☐	☐
The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1).	☒	☐	☐	☐

No VDP in "how to use your product securely", a webpage with poor accessibility
Source: https://support.polar.com/en/how-to-use-your-polar-product-securely



HOW TO USE YOUR POLAR PRODUCT SECURELY

Any security issues can be reported to security(a)polar.com or to Polar Customer Care.

Recommendations

We propose several recommendations to optimize the accessibility and usability of VDP in consumer IoT. By following them, manufacturers will improve the accessibility and usability of their VDP and its effectiveness.

R1. Implement global VDP strategy ("one VDP")

One of the biggest challenge IoT manufacturers are facing today is the regulatory overhead. A compliance-based approach can only cater to individual regulations, which will lead to potential gaps and issues. For instance, the EU RED DA does not require a VDP.

We recommend designing and implementing a global VDP strategy for consumer IoT products ("one VDP"). This "one VDP" should be the unique reference for external vulnerability reporters and for internal stakeholders: all products, all brands and all markets should have the same rules.

When designing their "one VDP", manufacturers must integrate all relevant regulatory requirements as well as internal constraints (for example, dedicated product security teams per brand or per market).

R2. Have a link to the VDP in the footer menu

The most common way for accessing a VDP is in the footer menu. This link would generally point to the VDP or to a dedicated product security website.

We recommend placing a link to the VDP in the footer with a self-explaining text such as "report a vulnerability" or "product security". Manufacturers should not place this link under any non-intuitive page such as the privacy notice, legal & compliance, support or FAQ.

R3. Keep the VDP open and public

The VDP and the point of contact must be clear and accessible freely. This is particularly true to comply with regulations in the UK and in the EU.

We recommend all manufacturers to keep their VDP open and public. This means removing login requirements and any other pre-requisite. This recommendation also applies to third-party platforms used for reporting.

R4. Have a valid security.txt

Manufacturers can place their VDP on any URL. This means that vulnerability reporters must navigate on a website and look for links to the VDP before submitting their findings. This study has highlighted several issues associated to this approach.

Manufacturers should formalise their VDP information in a `security.txt` file, and place it in the `.well-known/` directory of their product website. This will improve VDP accessibility by giving direct access to the relevant VDP information.

At cetome, we support the deployment of security.txt on products websites and on the corporate website. It brings immediate benefits with a low level of effort for implementation and maintenance.

R5. Make it easy to reach the point of contact

The point of contact should remain easy to reach, within an acceptable number of click and with no additional requirements. For example, reporters should not have to create an account.

R6. Prefer a webform for vulnerability reporting

A webform is the easiest way to implement a template and automate its treatment. It is easier to manage than emails with PGP and it could improve security by removing file attachments. Moreover, manufacturers who use binary files can easily convert them into a webform.

For more information, please refer to ETSI TR 103 838 which requires a reporting webform.

R7. Integrate VDP accessibility in standards and regulations

Standard development organisations ("SDOs") should develop requirements for VDP accessibility and usability. This is important as they are at the basis of several regulations (and probably of the future harmonised European Standard ("hEN") for the Cyber Resilience Act).

> Example of requirement to include in IoT cyber security standards:
>
> The vulnerability disclosure policy and the "point of contact" must be accessible easily and publicly.

R8. Follow web accessibility best practices

The VDP is almost always a public webpage. In several occasions, we found accessibility issues that could limit reporting and lead to a non-compliance.

We recommend all manufacturers to follow best practices for web accessibility. This includes user experience and making their VDP accessible on all platforms / browsers.

Acknowledgements

We would like to acknowledge David Rogers, the CopperHorse Limited team and the IoTSF for their yearly report on IoT VDP.

Future work

To continue this study, it would be interesting to look at statistics and trends regarding VDP accessibility and usability, by sector, by geography, by revenue, etc.

Another extension would be to analyse the content of the VDP and its compliance with standards and regulations.

Similar work could take place for product security advisories and their accessibility.

Additionally, the results of this study could contribute to the work on dynamic cyber security labels. These labels could check the VDP accessibility and usability as part of their requirements.

Conclusions

VDP is an important tool for improving the cyber security of consumer IoT products. In this study, we discovered that VDP accessibility is often overlooked. Indeed, having a VDP is not sufficient: it must be easy to access it and to submit reports.

We have identified multiple issues that could limit the effectiveness of a VDP. We proposed several recommendations including a global VDP strategy for all products, brands and markets ("one VDP"), a direct link in the footer menu and the implementation of a valid **security.txt**. Additionally, we believe that standard development organisations should integrate the concepts of accessibility and usability in their relevant standards.

At cetome, we promote VDP accessibility and usability in consumer IoT. This is an important area of work and it is now a regulatory requirement in several markets. For that purpose, we encourage all manufacturers to review their current approach and follow our recommendations.

To evaluate the accessibility of a vulnerability disclosure policy, we have developed a free "VDP Accessibility Scoring" tool accessible at cetome.com/vdp/score.

About this study

The study took place between July 2023 and January 2024. It was entirely self-funded.

About cetome

cetome is an independent cyber advisory with a recognised expertise in IoT security. We work with IoT manufacturers to embed security-by-design in their products, train their teams and improve their cyber resilience. This includes the development of accessible and usable vulnerability disclosure policies.

cetome
we make cyber work

CETOME

124 City Road
London, UK, EC1V 2NX

37 Rue Antoine CHARIAL
69003 Lyon, France

Email: info@cetome.com

Website: cetome.com