Vulnerability Disclosure Procedure - Beko Europe

About Beko Europe

Beko Europe is a leading home appliances business, dedicated to changing the lives of our customers through a wide range of innovative and sustainable household products and solutions. It was established in 2023 as a result of an agreement between Arçelik and Whirlpool, with Arçelik owning 75 percent of the company and Whirlpool owning 25 percent. It benefits from more than 60 years of leadership, innovation and expertise in the home appliance sector.

With more than 20,000 employees, Beko Europe has 69 subsidiaries and 11 production sites across Europe, which are located in Cassinetta, Melano, Comunanza, and Siena in Italy, Wroclaw, Radomsko, and Lodz in Poland, Poprad in Slovakia, Yate in the UK, and Ulmi and Gaesti in Romania, with a production capacity of approximately 24 million white goods products per year.

Established in the UK in 1990, Beko Europe is part of large multinational group - KOÇ Holdings and the consumer durables division, Arçelik. KOÇ Holdings is included in the Global Fortune list as one of the top 500 companies in the world.

1. Purpose

This Vulnerability Disclosure Procedure (VDP) provides guidelines for cybersecurity research to improve the security of our networked products, apps, and cloud services. This VDP also instructs researchers on how to submit discovered vulnerabilities to the relevant team. Please see here our brands, products and scope of Beko Europe.

2. Overview

We take security issues extremely seriously at Beko Europe and welcome feedback from security research to improve the security of our networked products, apps, and cloud services. We operate a procedure of coordinated disclosure for dealing with reports of security vulnerabilities and issues. Vulnerabilities submitted to us under this procedure will be used for defensive purposes to mitigate or remediate vulnerabilities in our networks and services.

Researchers must review and comply with the following terms and conditions of this VDP before conducting any research or testing on our networked products, apps and cloud services.

3. Guidelines

3.1. *Reporting a Suspected Security Issue*

If your discovered vulnerability is about one of our IoT products, is related to mobile applications or their related cloud services please send your report to psirt@homewhiz.com.

Please share the security issue with us before making it public on message boards, mailing lists, or other forums.

To receive credit, you must be the first to report a vulnerability, and you must notify us in accordance with the following:

You should provide basic details of the discovered issue, typically;

- Name/type of affected product/app/service, plus specific model number, serial number, etc.
- Any Proof of Concept(POC) setup details
- Description of the steps to reproduce the issue
- Public references if there are any
- The details of the system where the tests were conducted

By following the Vulnerability Disclosure Procedure, we will respond to you within a maximum of 48 business hours of receiving the initial report. If the reported security issue will be confirmed by looking at the impact, severity, and exploit the complexity of the vulnerability report; we may ask for your further contribution to resolve the potential vulnerability within 90 days.

3.2. *Scope of Vulnerabilities*
3.2.1. Accepted Vulnerabilities
We are willing to be informed about demonstrated vulnerabilities of medium/high impact, such as authentication/authorization, cryptography, data leakage, and URL redirector abuse.

3.2.2. *Out of Scope Vulnerabilities*

- SSL vulnerabilities related to configuration or version
- Denial of Service (DoS)
- User enumeration/Brute forcing (for example Login and Forgot Password page)
- HTTP Trace method is enabled.
- These qualify if you are able to execute an attack.
- Clickjacking on pages without any authentication and/or sensitive state changes
- Social Engineering/Phishing
- Content spoofing
- Self-XSS. Cross-site scripting issues should be exploitable in reflected, stored or DOM-based types.
- Logout and other instances of low-severity CSRF
- Missing HTTP headers
- Missing cookie flags on cookies
- Password complexity and reset password flow complexity
- Invalid or missing SPF (Sender Policy Framework) records
- Software banner/version disclosure.
- These qualify if you are able to provide an exploitable POC.
- Results of automated tools or scanners
- Autocomplete attribute on web forms
- Vulnerabilities which require a jailbroken device

Although we find every vulnerability that comes from you valuable, we ask you to stay away from any kind of security research that may harm our users, systems and services and has the possibility of data corruption. Also, if a researcher determines a vulnerability which includes any sensitive data (including personally identifiable information, financial information, or the proprietary information or trade secrets of any party), they must stop testing, notify the relevant e-mail address immediately through our vulnerability submission process, and not disclose this data to anyone else. If a researcher engages in any activities that are inconsistent with this procedure or other applicable laws, the researcher may be subject to criminal and/or civil liabilities.

3.3. *Disclosure of Vulnerability*
Public disclosure of vulnerabilities approved/processed by us is not permitted under any circumstances.

4. What you can expect from us

As Beko Europe, we will take appropriate steps to mitigate the risk and remediate the reported vulnerabilities by taking into account any vulnerabilities we receive and complying with the guideline.

Beko Europe commits to cooperating with security researcher(s) as transparently and quickly as possible.

If the researcher conducts vulnerability disclosure activities in accordance with our guidelines and applicable law, Beko will not initiate any law enforcement related to such activities.

5. Questions

If you have any questions about the guideline or the process, do not hesitate to contact us at psirt@homewhiz.com for IoT products.