Dometic Vulnerability Disclosure No. 1/2025

Introduction

Dometic welcomes feedback from security researchers and the general public to help improve our security. If you believe you have discovered a vulnerability, privacy issue, exposed data, or other security issues in any of our assets, we want to hear from you. This policy outlines steps for reporting vulnerabilities to us, what we expect, what you can expect from us.

Official Channels

To report a security vulnerability, please contact us via e-mail:

- E-Mail: productcybersecurity@dometic.com

Systems in Scope

This policy applies to any digital appliance manufactured by Dometic.

Out of Scope

Appliances or other equipment not manufactured by Dometic are out of scope of this policy.

Our Commitments

You can expect from us to:

- Respond to your report promptly, and work with you to understand and validate your report;
- Strive to keep you informed about the progress of a vulnerability as it is processed;
- Work to remediate discovered vulnerabilities in a timely manner, within our operational constraints; and
- Extend Safe Harbor for your vulnerability research that is related to this policy.

Our Expectations

In participating in our vulnerability disclosure program in good faith, we ask that you:

- Play by the rules, including following this policy and any other relevant agreements. If there is any inconsistency between this policy and any other applicable terms, the terms of this policy will prevail;

- Report any vulnerability you've discovered promptly;
- Help us improve efficiency evaluating and resolving the vulnerability by giving us relevant information such as assets (web address, IP address, product or service name), description of vulnerability (including summary, steps to reproduce, supporting files) and assessed impact (what could and attacker do using this vulnerability);
- Avoid violating the privacy of others, disrupting our systems (e.g., DoS or DDoS), destroying data, and/or harming user experience;
- Use only the Official Channels to discuss vulnerability information with us;
- Provide us a reasonable amount of time (at least 90 days from the initial report) to resolve the issue before you disclose it publicly;
- Perform testing only on in-scope systems, and respect systems and activities which are out-of-scope;
- If a vulnerability provides unintended access to data: Limit the amount of data you access to the minimum required for effectively demonstrating a Proof of Concept; and cease testing and submit a report immediately if you encounter any user data during testing, such as Personally Identifiable Information (PII), Personal Healthcare Information (PHI), credit card data, or proprietary information;
- You should only interact with test accounts you own or with explicit permission from the account holder; and
- Do not engage in extortion.

Irrelevant Vulnerabilities

Issues that we do not consider relevant vulnerabilities include, but are not limited to:

- Missing security features alone without demonstrated impact
- Missing rate limiting without demonstrated impact
- Missing security-related HTTP headers without demonstrated impact
- Missing or incomplete SPF/DKIM/DMARC records
- Content spoofing without demonstrated impact
- Automated scan reports without proof-of-concept or explanatory documentation
- Clickjacking and issues that are only exploitable through clickjacking
- Self-XSS
- Social engineering attacks

Safe Harbor

When conducting vulnerability research, according to this policy, we consider this research conducted under this policy to be:

- Authorized concerning any applicable anti-hacking laws, and we will not initiate or support legal action against you for accidental, good-faith violations of this policy;
- Authorized concerning any relevant anti-circumvention laws, and we will not bring a claim against you for circumvention of technology controls;

- Exempt from restrictions in our Terms of Service (TOS) and/or Acceptable Usage Policy (AUP) that would interfere with conducting security research, and we waive those restrictions on a limited basis; and
- Lawful, helpful to the overall security of the Internet, and conducted in good faith.

As long as you comply with this policy, we will honor the Safe Harbor Policy, as defined below:

- We refrain from filing a charge to the national laws
- If legal action is initiated by a third party against you and you have complied with this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.

If at any time you have concerns or are uncertain whether your security research is consistent with this policy, please submit a report through one of our Official Channels before going any further.

Note that the Safe Harbor applies only to legal claims under the control of the organization participating in this policy, and that the policy does not bind independent third parties.