belkin

Product Vulnerability Disclosure Policy

Product Vulnerability Disclosure Policy

April 14, 2026

Introduction

Belkin is committed to ensuring the security of our products and other assets for the protection of our customers. This policy is intended to assist security researchers and others by setting out how we consider that vulnerability discovery activities can best be carried out, to convey our preferences in how to report discovered vulnerabilities to us, and to inform you as to how and when you can expect us to respond to any such report.

We encourage you to contact us to report potential vulnerabilities in our systems, by using the Vulnerability Disclosure Form which you will find here: https://belkin.my.salesforce-sites.com/caforms/VulnerabilityDisclosureForm

Once you report a potential vulnerability to us, we will acknowledge receipt within the next 10 business days. We will diligently investigate your report, and keep you updated on significant developments. In any event we will inform you within 20 business days of concluding our investigation.

We commit to coordinating with you as openly and as quickly as possible. To the extent appropriate we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including on issues or challenges that may delay resolution. We will maintain an open dialogue to discuss issues.

Guidelines

If you are engaged in vulnerability research or if you otherwise consider that you have discovered a Belkin security vulnerability, we request that you:

- Notify us as soon as possible after you discover a real or potential security issue, using our Vulnerability Disclosure Form at https://belkin.my.salesforce-sites.com/caforms/VulnerabilityDisclosureForm
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data
- Only use exploits to the extent necessary to confirm a vulnerability's presence. Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems
- Provide us a reasonable amount of time to resolve the issue before you disclose it publicly
- Do not submit a high volume of low-quality reports.

If you access any sensitive data (including personally identifiable information, financial information, or proprietary information or trade secrets of any party), we request that you **stop your test, notify us immediately, and do not disclose this data to anyone else**.

Test methods

The following test methods are not authorized, may be unlawful and could result in action being taken against you:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data
- Physical testing (e.g. office access, open doors, tailgating), social engineering (e.g. phishing, vishing), or any other non-technical vulnerability testing

Scope

This policy applies to the following products, services and systems:

- Products sold and currently supported by Belkin that incorporate Ethernet, Wi-Fi, or other Internet Protocol-based network interfaces
- Belkin internet-connectable and network-connectable products sold in the UK that Belkin has declared to be in compliance with the UK Product Security and Telecommunications Infrastructure Act 2022
- Software and applications published by Belkin and required for use of Belkin products

This policy does not apply to:

- Belkin.com web endpoints
- Any unlawful activity including activities such as those referred to above
- Belkin-branded Wi-Fi routers and range extenders; these products are produced and supported by Linksys (www.linksys.com)

Any product or service not provided by Belkin, such as any connected services, are excluded from scope and Belkin does not authorize them for testing. Vulnerabilities found in any third-party product, service or system should be reported directly to the third party concerned.

Reporting a Vulnerability

Information submitted under this policy will be used for to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service, we may share your report with the appropriate governmental authorities, including the U.S. Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without your permission, unless otherwise required by law.

What we would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the conditions under which the vulnerability was discovered and the potential impact of exploitation
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of photos, videos. concept scripts, or screenshots are helpful)
- Be provided in English, if possible

Questions

Questions regarding this policy may be sent to **cvdp@belkin.com.** We also invite you to contact us with suggestions for improving this policy.

Document change history

Version	Date	Description
1.0	July 24, 2024	First issuance.
1.1	March 31, 2025	Updated e-mail address.
1.2	April 14, 2026	Various minor updates; removal of references to deprecated Wemo products and services