Vulnerability Disclosure Policy

Loewe Technology GmbH, 96317 Kronach , Germany
Revision: 1.2 by MM

Introduction

This vulnerability disclosure policy applies to any vulnerabilities you are considering reporting to us. We recommend reading this policy fully before you report a vulnerability and always acting in compliance with it. We value those who take the time and effort to report security vulnerabilities according to this policy. For repeated vulnerabilities in the same time period, the first most complete report shall prevail, and for repeated vulnerabilities in different time periods, the first submission shall prevail. We do not offer monetary rewards for vulnerability disclosures.

Reporting

If you believe you have found a security vulnerability, submit your report to us using the following link email: helpline@loewe.de. In your report please include:

- Model number on which the vulnerability can be observed
- Title of vulnerability (mandatory)
- Description of vulnerability (this should include a summary, supporting files and possible mitigations or recommendations) (mandatory)
- Impact (what could an attacker do?) (mandatory)
- Steps to reproduce. These should be a benign, non-destructive, proof of concept. This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports, or malicious exploitation of some vulnerabilities, such as sub-domain takeovers.
- Contact Information. If you would like us to follow-up with you with status reports, please provide us with sufficient contact information, such as contact name and email address, so that we can keep in touch with you. You are not required to provide contact information to submit a report. Please note your contact information will only be used to contact you regarding the vulnerability you reported and will not be used for any other purpose. Your personal information will be protected as described in Privacy Policy (https://www.loewe.tv/privacy-policy)

What to expect

After you have submitted your report, and if you provide contact information, we will respond to your report within 7 calendar days to acknowledge the receipt of your report and aim to triage your report within 15 working days. Statutory holidays or vulnerability outbreaks may slow down the response time. We'll also keep you informed of our progress, including:

- Status update of your report.
- Significant new information regarding to your report.
- Changes to existing fix plans.
- Disclosure plans, if any

Priority for remediation is assessed by looking at the **impact, severity and exploit complexity**.

Critical risk vulnerabilities will be patched within 7 working days after the assessment is completed. **High and medium risk** vulnerabilities will be fixed within 30 working days. **Low-risk** vulnerabilities will be fixed within 180 working days. Please note that some vulnerabilities are dependent on environment or hardware. The final fixing time will be determined according to the actual situation.

You are welcome to enquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation. We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the solution covers the vulnerability adequately. Once your vulnerability has been resolved, we welcome requests to disclose your report. We'd like to unify guidance to affected users, so please do continue to coordinate public release with us.

Vulnerability Level Rating Criteria

<u>Critical Risk Vulnerabilities:</u>

1. Direct access to core system permissions. Vulnerabilities that can directly endanger the intranet, including but not limited to: command execution, remote overflow and other vulnerabilities;

2. Vulnerabilities that can obtain a large number of core user data;

3. Logical loopholes that have direct and serious impacts. Vulnerabilities include but are not limited to: serious logic errors, loopholes that can obtain a large amount of benefits and cause losses to companies and users.

<u>High Risk Vulnerabilities:</u>

1. Vulnerability of directly obtaining business server permissions. Including but not limited to arbitrary command execution, uploading webshell, arbitrary code execution, command injection, remote command execution;

2. Logical loopholes that have direct and serious impacts. Including but not limited to any account password change vulnerability;

3. Vulnerabilities that can directly steal user identity information in batches. Including but not limited to SQL injection;

4. Unauthorized access. Including but not limited to bypassing authentication to directly access the administrator back end, and weak passwords in the back end.

<u>Medium Risk Vulnerabilities:</u>

1. The vulnerability of directly obtaining user identity information. Including but not limited to stored XSS vulnerabilities;

2. Arbitrary text operation loopholes. Including but not limited to any file reading, writing, deleting, downloading and other operations;

3. Unauthorized access. Including, but not limited to modifying user data, and performing user operations by circumventing restrictions;

<u>Low Risk Vulnerabilities:</u>

1. Vulnerabilities that can have certain impact but cannot directly obtain device permissions and affect data security, such as: non-important information disclosure, URL redirection, difficult-to-use XSS security vulnerabilities, common CSRF vulnerabilities.

2. Ordinary unauthorized operation. Including but not limited to incorrect direct object references.

3. Common logic design flaws. Including but not limited to SMS verification code bypass, email verification bypass.

The following issues are not vulnerabilities:

1. Bugs that do not involve security issues. Including but not limited to product functional defects, garbled web pages, confusing styles, static file directory traversal, application compatibility and other issues.

2. Vulnerabilities that cannot be exploited. CSRF without sensitive operations, meaningless abnormal information leakage, intranet IP address/domain name leakage.

3. Other problems that cannot directly reflect the existence of vulnerabilities. Including, but not limited to, issues that are pure guesswork.

Guidance

You must NOT:

- Break any applicable law or regulations.
- Access unnecessary, excessive or significant amounts of data.
- Modify data in the organization's systems or services.
- Use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Attempt or report any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Disrupt the organization's services or systems.

Security Support Period

We take the growing risk of security threats to our products very seriously. We have long been committed to the ongoing effort to continuously provide security updates for our products. Device models will be supported with security updates for at least 2 years from their launch day. If a security vulnerability with extremely high risk is disclosed, we may still provide necessary security updates to you, even if your device is in the EOL product list.

Launch Date for Products

Model number	*Model name*	*Launch date*	*Sales-End date*	*Support period*	*Support end date*
60431 xxx 60433 xxx 60435 xxx 60437 xxx	Loewe bild i	2021-06-01	2024-07-01	4 years	2025-07-01
64548 xxx 64555 xxx 64565 xxx	We. SEE oled	2024-06-20	2027-06-20	4 years	2028-06-20
62463 xxx 62464 xxx 62466 xxx 62466 xxx	Loewe inspire	2024-06-20	2027-06-20	4 years	2028-06-20
63407 xxx 63409 xxx	Loewe callas	2024-06-20	2027-06-20	4 years	2028-06-20
63532 xxx 63543 xxx	We. SEE lcd	2024-06-20	2027-06-20	4 years	2028-06-20
64510 D10	We. BEAM	2024-07-01	2028-07-01	5 years	2029-07-01
63465 xxx 63466 xxx 63469 xxx 63470 xxx 63474 xxx 63477 xxx 63478 xxx	Loewe stellar	2024-07-01	2027-12-31	5 years	2029-12-31