LuxBalance Lighting responsible disclosure statement

LuxBalance Lighting is committed to ensuring the safety and security of customers who use our products and services. LuxBalance Lighting maintains a network of security experts for developing and deploying best practice security features for our products and services, as well as for managing security events. *LuxBalance Lighting operates under a global product security policy.* LuxBalance Lighting supports coordinated vulnerability disclosure, and also encourages responsible vulnerability testing by security researchers and by customers, with responsible reporting to LuxBalance Lighting.

When submitting reports of vulnerability findings, please ensure the following procedure is followed, for safe and efficient support.

Reporting Procedure:

1. Please email submissions to us at productsecurity@luxbalancelighting.com.
2. Please provide us with your reference/advisory number and sufficient contact information, such as your organization and contact name so that we can get in touch with you.
3. Please provide a technical description of the concern or vulnerability.
    1. Please provide information on which specific product you tested, including product name and version number; the technical infrastructure tested, including operating system and version; and any relevant additional information, such as network configuration details.
    2. For web based services, please provide the date and time of testing, URLs, the browser type and version, as well as the input provided to the application.
4. To help us to verify the issue, please provide any additional information, including details on the tools used to conduct the testing and any relevant test configurations. If you wrote specific proof-of-concept or exploit code, please provide a copy. Please ensure all submitted code is clearly marked as such.
5. If you have identified specific threats related to the vulnerability, assessed the risk, or have seen the vulnerability being exploited, please provide that information.
6. If you communicate vulnerability information to vulnerability coordinators such as ICS-CERT, CERT/CC, NCSC or other parties, please advise us and provide their tracking number, if one has been made available.

Product Security Vulnerability Report Assessment and Action:

1. LuxBalance Lighting will acknowledge receiving your report within two business days.
2. LuxBalance Lighting will provide you with a unique tracking number for your report.
3. LuxBalance Lighting will assign a contact person to each case.
4. LuxBalance Lighting ’s central security incident response team will notify the appropriate product teams.
5. LuxBalance Lighting will keep you informed on the status of your report.
6. If the vulnerability is actually in a third party component or service which is part of our product/service, we will refer the report to that third party and advise you of that notification. To that end, please inform us in your email whether it is permissible in such cases to provide your contact information to the third party.
7. Upon receiving a vulnerability report, LuxBalance Lighting will:
    1. Verify the reported vulnerability.
    2. Work on a resolution.
    3. Perform QA/validation testing on the resolution.
    4. Release the resolution.
    5. Share lessons learned with development teams.
8. LuxBalance Lighting will use existing customer notification processes to manage the release of patches or security fixes, which may include without limitation and at LuxBalance Lighting’s sole discretion direct customer notification or public release of an advisory notification on our website.

Important:

1. Refrain from including sensitive personal information in any screen shots or other attachments you provide to us. Make a good faith effort not to access or destroy another user's data.
2. Do not perform any vulnerability or similar testing on applications, products or services that are actively in use. Vulnerability testing should only be performed on devices or applications, products or services not currently in use or not intended for use.
3. For web bases applications, products or services, please use demo/test environments to perform vulnerability testing.
4. Do not take advantage of the vulnerability or problem you have discovered; for example, by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying any data.
5. After vulnerability testing, each device should be retested to ensure no damage has been inflicted and the device is suitable for use. In case the application, product or service is serviced by a provider, then please contact your service provider prior to the device being placed back into use.
6. As part of responsible co-ordination of vulnerability disclosure, we encourage you to work with LuxBalance Lighting on selecting public release dates for information on discovered vulnerabilities. To minimize the possibility of public safety, privacy and security risks, we request your cooperation in synchronizing the release of information. Please inform us of your disclosure plans, if any, prior to public disclosure.
7. The discloser’s actions must not be disproportionate, such as, including without limitation:
    1. Using social engineering to gain access to the application, product or service.
    2. Building his or her own backdoor in an information application, product or service with the intention of then using it to demonstrate the vulnerability, as doing so can cause additional damage and create unnecessary security risks.

    3. Utilizing a vulnerability further than necessary to establish its existence.
    4. Copying, modifying or deleting data on the application, product or service. An alternative for doing so is making a directory listing of the application, product or service.
    5. Making changes to the application, product or service.
    6. Repeatedly gaining access to the application, product or service or sharing access with others.
    7. Using brute force attacks to gain access to the application, product or service. This is not a vulnerability in the strict sense, but rather repeatedly trying out passwords.

8. LuxBalance Lighting will provide full credit to researchers who make a vulnerability report or perform testing, in publicly released patch or security fix release information, if requested.

Notice:

In case you decide to share any information with LuxBalance Lighting, you agree that the information you submit will be considered as non-proprietary and non-confidential and that LuxBalance Lighting is allowed to use such information in any manner, in whole or in part, without any restriction. Furthermore, you agree that submitting information does not create any rights for you or any obligation for LuxBalance Lighting.

Last update: 10 January 2019