Philips Projection coordinated vulnerability disclosure statement

Last updated: 04 July 2024

Philips projection (Screeneo Innovation SA) is committed to ensuring the safety and security of patients, operators and customers who use our products and services. Philips projection maintains a global network of product security officers for developing and deploying advanced best practice security and privacy features for our products and services, as well as for managing security events.

If you believe you have discovered a vulnerability in a Philips Projection product or have a security incident to report, please fill out the vulnerability report form https://support.philipsprojection.com/hc/en-us

When we receive a vulnerability report, Philips projection takes a series of steps to address the issue internally, referring to ISO/IEC 30111. All reported vulnerabilities are scored according to the Common Vulnerability Scoring System 3.1 (CVSS) standard.

Reporting Procedure

1. Please contact email submissions to us at philips.projector.eu@screeneo.com if any hardware and software questions.
2. Please provide a technical description of the concern or vulnerability.
a) 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.
b) 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.
3. 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.
4. If you have identified specific threats related to the vulnerability, assessed the risk, or have seen the vulnerability being exploited, please provide that information.
5. 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.
6. When possible provide the report in English to expedite the process.

Product Security Vulnerability Report Assessment and Action

1. Philips projection will acknowledge receiving your report within 7 calendar days and provide you with a unique tracking number for your report.

2. Upon receiving a vulnerability report, Philips projection will:
a) Verify the reported vulnerability.
b) Work on a resolution.
c) Perform QA/validation testing on the resolution.
d) Release the resolution.

3. Philips projection will use existing customer notification processes to manage the release of patches or security fixes such as OTA releases (over the air) which may include direct customer notification or public release of an advisory notification on our website.

Critical risk vulnerabilities will be fixed within 7 business days.

High and medium risk vulnerabilities will be fixed within 30 business days.

Low risk vulnerabilities will be fixed within 180 business days.

Note, some vulnerabilities are subject to environment or hardware restrictions. Final remediation time will be determined according to the real-world situation. We will provide status updates as soon as possible until the issue is resolved.

We greatly appreciate anyone who can give us a chance to improve our products and services, and better protect our users.

Thank you for working with us through the above process.