Milestone cybersecurity development policy

Introduction

The Milestone cybersecurity policy is a document describing the objectives, procedures and controls that ensure that Milestone and its customers have a clear understanding of the risks and measures in place regarding cybersecurity in the development, deployment and integration with the Milestone XProtect® portfolio of products.

Scope

This document describes the development procedures within the R&D and Support department.
The policy consists of three elements:

1) Development procedures
2) Documentation and other proactive measures
3) Cybersecurity response planning

Development procedures

Milestone software development is conducted per the Milestone Secure Development Lifecycle, inspired by the Microsoft Secure Development Lifecycle (https://www.microsoft.com/en-us/sdl/default.aspx).

The key requirements regarding development under the Milestone SDL are:

a. Follow best practices
   Use OWASP top 10 lists to ensure that we have the most common threats mitigated.
b. Secure by design
   Design for security, eliminating less secure legacy code and doing threat modelling.
c. Secure by default
   Apply principles as “defense in depth”, “least privileges” and avoid less secure default settings and turn off infrequently used features by default.
d. Secure by deployment
   Ensure that the documentation provided supports our partners in adequately securing customers’ installations, mainly through the hardening guide.

1) Threat modelling is done and documented to clarify and register the threats and mitigations exposed by the functionality.

2) Security Testing is carried out and documented, both white box and black box

   a. Penetration testing
   b. Fuzz testing

3) All members of the R&D department undergo annual training in cybersecurity development and testing relevant to their discipline.

4) The SDL and this policy is reviewed once a year, and the current revision of this document was updated on March 1, 2019.

Documentation and other proactive measures

As described in the SDL, the documentation of cybersecurity considerations and descriptions are done through threat modelling. The process is done as part of the refinement and throughout the implementation phase of the development cycle.

Cybersecurity response planning

The reactive part of the cybersecurity policy consists of three types of incidents:

1) Milestone becomes aware of a vulnerability in released software
2) A customer/partner makes Milestone aware of a potential vulnerability in released software
3) An attack is allegedly successful in damaging/threatening Milestone and or a customer/ partner's installation/reputation etc.

In order to be prepared for this type of eventualities, we will:

1) Document all third-party libraries used in our released products, both open source and licensed, and register these in a third-party database in order to get notifications regarding possible threats and vulnerabilities.
2) Release management will monitor previous releases in a similar manor, to detect if any vulnerabilities have been discovered and published through the risk database. Bugs will be created to allow the feature team and the Milestone cybersecurity team to perform triage.
3) Prior to each release, a review of the current version of third-party components will be performed, to determine if any revision updates should be considered from a cybersecurity point of view.
4) In the case of a critical zero-day vulnerability, we will publish the information regarding the vulnerability and the mitigation on our cybersecurity webpage as soon as the information is available, using our hotfix process for distribution of the components.

Our cybersecurity webpage informs our partners and customers about our policies. Partners and customers can get in touch with the Milestone cybersecurity team via cybersecurity@milestone.dk and get a response within 48 hours.