MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS

Vulnerability Management Policy

milestone

Contents

Purpose

Milestone (“we,” “our,” or “us”) collects, discloses and resolves product vulnerabilities to ensure the security of our products and services, and to protect our customers from cyber threats. When vulnerabilities are discovered, either by Milestone development teams or external security researchers, Milestone will work diligently to investigate, disclose and resolve them according to this vulnerability management policy.

Overview

As a **CVE Numbering Authority (CNA) under the MITRE domain,** Milestone follows the industry's best practices in managing and responding to security vulnerabilities discovered in our products.

As with any software product or service, it is a general condition that it is impossible to guarantee that the software is completely free from vulnerabilities. However, as described in our SDL, Milestone can guarantee that we make a thorough effort to identify and mitigate potential vulnerabilities in our software, reducing the customer's risk of deploying or using Milestone's software products or services in their environment.

Milestone acknowledges that standard network protocols and the Microsoft Windows operating system may have inherent weaknesses that might be exploited. While Milestone does not take the responsibility for vulnerabilities in standard network protocols and Microsoft's Windows operating systems, we do provide recommendations on how to reduce the risks related to using Milestone products and services in your IT infrastructure. See the XProtect VMS hardening guide, XProtect VMS certificates guide, Whitepaper - Ensuring end-to-end protection of media integrity, and eLearning - Ensuring Secure Systems.

Vulnerability Reporting and Milestone Commitment

Milestone appreciates and encourages efforts made by researchers in identifying and reporting vulnerabilities for Milestone products and services. By following the vulnerability-disclosure process described in this policy, Milestone's Product Security Team will, to the best of our abilities, respect the researcher's interests through mutual transparency and collaboration throughout the disclosure process.

Milestone expects researchers not to disclose identified vulnerabilities until at least 90 days after the vulnerability has been communicated to Milestone, or, alternatively, not before a mutually agreed date. Milestone also expects vulnerability researchers to perform their research within legal boundaries that would not cause harm, expose privacy, or in general compromise the safety of Milestone, our partners and customers.

Reporting vulnerabilities

Milestone continuously work to identify, limit, and address the risks associated with vulnerabilities in our products and services. However, should you identify a security vulnerability in a Milestone product or service, we encourage you to report the vulnerability to Milestone immediately. The process of speedy communication of identified security vulnerabilities is critical to reduce the likelihood and time period a vulnerability might be exploited in practice.

Any person who has identified a potential vulnerability in Milestone's products and services can securely and confidentially Contact Milestone's security response team. You can submit the form with your contact details for further contact and communication with you about the vulnerability, or submit the form anonymously if you want to. Regardless of your choice, all data submitted is handled according to our Privacy Policy.

No matter if the form is submitted with contact details or anonymously, we require you to inform us of which product and version or service the vulnerability have been found in. You must also provide a title and description of the vulnerability. If you have files that document or support the described vulnerability, you can upload them as part of the submission.

For submissions that are not anonymous, Milestone will confirm the vulnerability submission within two (2) business days, and triage the submitted vulnerability within 15 business days.

Compensation

Milestone does not compensate researchers for any vulnerabilities or weaknesses reported to us.

In Scope Vulnerabilities

The vulnerability management policy described in this document applies to all Milestone-branded products and services.

Out-of-scope vulnerabilities

Some vulnerabilities are considered outside the Milestone vulnerability management policy. Please don't report on the below vulnerabilities:

- Unsupported products or services that have reached the "Terminated" state
- Vulnerabilities in third-party plug-ins or integrations, for example plug-ins installed in the VMS' event server or clients.
- DLL-hijacking/DLL-sideloading vulnerabilities for Milestone products running on Microsoft Windows operating systems. For more information, see the following article.
- User misconfiguration that could be prevented by following Milestone guides, training, and best practice recommendations:
    - XProtect VMS hardening guide
    - XProtect VMS certificates guide
    - eLearning - Ensuring Secure Systems
- Vulnerabilities that have highly privileged account permissions as a prerequisite.
- Vulnerabilities in Microsoft Windows.
- Vulnerabilities in any third-party software installed in Microsoft Windows

Vulnerability management

Milestone scores reported vulnerabilities using the industry vulnerability scoring system CVSSv3.1 Common Vulnerability Scoring System and provide patches according to the scores listed below.

In case the person reporting the vulnerability has disclosed their contact information, Milestone will collaborate with them on details, such as the CVSSv3.1 score, content of security advisory, and date for the external disclosure.

CVSSv3.1 critical (9.0 – 10.0)

Milestone aims to patch the vulnerability within two (2) months of validating the vulnerability. Patches are provided for all product versions in 'General availability' and 'Limited availability' at the time the patch is released.

CVSSv3.1 high (7.0 – 8.9)

Milestone aims to patch the vulnerability within three (3) months of validating the vulnerability. Patches are provided for all product versions in 'General availability'.

CVSSv3.1 medium/low (0.1 – 6.9)

Milestone aims to patch the vulnerability as part of a scheduled, upcoming release. Patches are not provided for already released products.

Disclosing vulnerabilities

When reported vulnerabilities have been investigated and validated to be a legitimate vulnerability that warrants public disclosure, Milestone assigns a CVE ID to the vulnerability and initiates the responsible disclosure process, which consists of submitting the CVE ID to MITRE, publishing information about the vulnerability on our cybersecurity web site, and, when applicable, publish a press release.

Milestone Product Lifecycle

The support for Milestone products is defined through the Milestone Product Lifecycle process.

Generally, Milestone releases new versions of our XProtect software products three times a year, where previous released versions change their status from General Availability to Limited Availability three months after a similar or substituting product has been released. In special cases where a newer version has not been released, Limited Availability will start one year from the General Availability date.

Milestone guarantees a minimal availability period of four years for all its VMS products, in which the product becomes Discontinued after three years from its General Availability date and Terminated after four years.

You can find the availability details, including available for new purchase, support, hotfixes, and more. for the products and versions at different product lifecycle stages here: Lifecycle for XProtect - retiring versions and Lifecycle for XProtect – retiring products

Find a complete list of Terminated products here: Terminated Products

helpfeedback@milestone.dk

About Milestone

Milestone Systems is a leading provider of open platform video management software; technology that helps the world see how to ensure safety, protect assets and increase business efficiency. Milestone Systems enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 150,000 sites worldwide. Founded in 1998, Milestone Systems is a stand-alone company in the Canon Group. For more information, visit https://www.milestonesys.com/.