MAKE THE
WORLD SEE

Milestone Systems

XProtect® VMS

Vulnerability Scanner Guide

milestone

Contents

Introduction

Vulnerabilities and risks

Vulnerability management is all about managing and reducing risks in IT systems.

Because all software might have vulnerabilities (known or unknown) it is impossible to completely ensure that all software and IT equipment used in an IT system have no vulnerabilities. However, by installing and configuring the network, servers, operating system, SQL server, cameras, and the XProtect VMS software in the right way, the risk of exploitable vulnerabilities is greatly reduced.

So, before you scan for and report vulnerabilities, you must follow our Milestone XProtect VMS Hardening Guide and Milestone XProtect Certificate Guide, which describe several security controls and recommendations that minimize the risks when deploying our XProtect VMS on the Microsoft Windows operating system.

If vulnerabilities, are found in the Milestone XProtect software and, potentially, Microsoft's Windows operating system and reported to Milestone, we use the commonly used CVSS (Common Vulnerability Scoring System) measure to determine the risk of the vulnerability and the CVSS score. Validated vulnerabilities are addressed according to our Vulnerability Management Policy.

In extent to responding to reported vulnerabilities, Milestone monitors the CVE (Common Vulnerabilities & Exposure) database for vulnerabilities related to the Microsoft Windows operating systems, and open-source packages used in the Milestone XProtect VMS software. Such identified vulnerabilities are also addressed according to our Vulnerability Management Policy.

Vulnerabilities typically reported by scanning tools

Microsoft Windows, SQL server and 3rd party software

Scanning tools typically try to identify known vulnerabilities by examining the version numbers of Microsoft Windows and other software products installed in Windows. This includes SQL server, virus scanner, and virus definitions, plus other third-party software installed in Windows.

In case the scanning tool reports vulnerabilities for Microsoft Windows, the SQL server, or other third-party software installed in Windows, please update or patch Windows and all other software products to newest versions. Also ensure that you have followed all recommendations in the Milestone XProtect VMS Hardening Guide , before scanning again for vulnerabilities.

If vulnerabilities are still reported for Microsoft Windows, SQL Server, or any third-party software, report the vulnerability to Microsoft or the vendor of the third-party software.

Unsecure services, ciphers and hashing functions

If the scanning tool has detected unsecure services, ciphers, or hashing functions, ensure that you have followed all recommendations in the Milestone XProtect VMS Hardening Guide and the Milestone XProtect Certificate Guide , including disabling none-essential Windows services, ciphers, and hashing functions.

Scanning tools might report that the communication on certain XProtect VMS ports still use HTTP, even when certificates have been configured for all the XProtect VMS servers. In this case, consult the XProtect VMS documentation on ports used by the XProtect VMS. Some XProtect VMS ports use Windows Communication Foundation (WCF) that offers message-based security and encryption, instead of transport-level security (HTTPS).

You can also use the documentation of the ports used by the XProtect VMS to identify which ports are used by the Milestone XProtect VMSm d by Microsoft Windows, by or third-party software.

Secure Communication

If the scanning tool reports issues with secure communication for XProtect services, follow the recommendations in the Milestone XProtect Certificate Guide.

In particular take the recommended actions for these issues:

- **Communication not encrypted**
  - Create or obtain valid certificates issued by a trusted external or internal certificate authority (CA), and apply them across all XProtect services/components and clients.

- **Certificate have expired**
  - Create or obtain valid certificates issued by a trusted external or internal certificate authority, and apply them across all XProtect services/components and clients.
- **Certificate uses weak ciphers and hash algorithms**
  - Create or obtain valid certificates issued by a trusted external or internal certificate authority that uses modern and secure ciphers and hash algorithms, and apply them across all XProtect services/components and clients.
- **Certificate are self-signed**
  - Add the computers to a Microsoft Active Directory (AD) Windows domain that can issue valid and trusted certificates. Then obtain AD-issued certificates and apply them across all XProtect services/components and clients.
  - Alternatively, install a Public Key Infrastructure (PKI) service, create valid and trusted certificates, and apply them across all XProtect services/components and clients.

Milestone XProtect VMS

If the scanning tool reports issues with the Milestone XProtect services/components, make sure that you have installed the latest version of XProtect VMS , and that you have followed the recommendations in the Milestone XProtect VMS Hardening Guide and Milestone XProtect Certificate Guide.

If vulnerabilities are still found after you have followed the information in the Milestone XProtect VMS Hardening Guide and Milestone XProtect Certificate Guide, please report the vulnerability to Milestone using our vulnerability form. Milestone investigate the reported vulnerability and address any validated vulnerabilities according to our Vulnerability Management Policy.

Camera and other equipment vulnerabilities

Vulnerabilities found in cameras, network equipment, network-attached storage systems, or other devices used in conjunction with the XProtect VMS, must be reported to the vendor of the equipment.

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/.