Vulnerability Management Policy - Arteco uSee / Uss

Contents

Purpose

Arteco (“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 Arteco development teams or external security researchers, Arteco will work diligently to investigate, disclose and resolve them according to this vulnerability management policy.

Overview

Arteco follows the industry's best practices in managing and responding to security vulnerabilities discovered in our products. While it is impossible to guarantee that software is completely free from vulnerabilities, Arteco commits to identifying and mitigating potential vulnerabilities, reducing the customer's risk of deploying or using Arteco’s software products or services.

Vulnerability Reporting and Arteco Commitment

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

Arteco expects researchers not to disclose identified vulnerabilities until at least 90 days after the vulnerability has been communicated to Arteco, or, alternatively, not before a mutually agreed date. Arteco 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 Arteco, our partners and customers.

Reporting vulnerabilities

Arteco continuously work to identify, limit, and address the risks associated with vulnerabilities in our products and services.

Any person who has identified a potential vulnerability in Arteco's products and services can securely and confidentially contact Arteco's security response team at security@arteco-global.com. Submissions should include product name, version, and a description of the vulnerability. Supporting documentation can also be attached.

Arteco will confirm the vulnerability submission within two (2) business days, and triage the submitted vulnerability within 15 business days.

Compensation

Arteco 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 Arteco-branded products and services.

Out-of-scope vulnerabilities

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

- Unsupported products or services that have reached End of Life
- Vulnerabilities in third-party plug-ins or integrations
- DLL-hijacking/DLL-sideloading vulnerabilities for Arteco products running on Microsoft Windows operating systems
- Vulnerabilities caused by user misconfiguration that could be prevented by following Arteco guides and best practices
- Vulnerabilities requiring highly privileged account permissions
- Vulnerabilities in Microsoft Windows or other third-party software

Vulnerability management

Arteco scores reported vulnerabilities using the Common Vulnerability Scoring System (CVSS) and provides patches according to severity:

- CVSS critical (9.0 – 10.0): Arteco aims to patch within two (2) months.
- CVSS high (7.0 – 8.9): Arteco aims to patch within three (3) months.
- CVSS medium/low (0.1 – 6.9): Arteco aims to patch in scheduled future releases.

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

Disclosing vulnerabilities

When reported vulnerabilities are validated, Arteco initiates a responsible disclosure process. Information is published on our cybersecurity section of the website, and, when applicable, through security advisories.

Arteco Product Lifecycle

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

Arteco releases new versions of uSee and uSS regularly. Products remain supported for at least four years, transitioning from General Availability to Limited Availability, then Discontinued and finally Terminated. Details on availability, support and updates are communicated through Arteco's official channels.

About Arteco

ARTECO is a company specialized for over 30 years in the design and development of software solutions for video surveillance and video management. It offers products and services that go beyond traditional video surveillance, both incoming and outgoing, and include advanced features such as video analytics, integration with other systems, process automation and video management.

Arteco, a global leader in the VMS platform sector, is present in Europe, North America, Latin America and Africa and supported by a network of certified distributors and partners present throughout the world.

For more information, visit https://www.arteco-global.com
Contact: support@arteco-global.com or security@arteco-global.com
LinkedIn: https://www.linkedin.com/company/arteco-global
YouTube: https://www.youtube.com/@ArtecoGlobal