Speco Technologies' Vulnerability Response Policy

July 2022

speco technologies

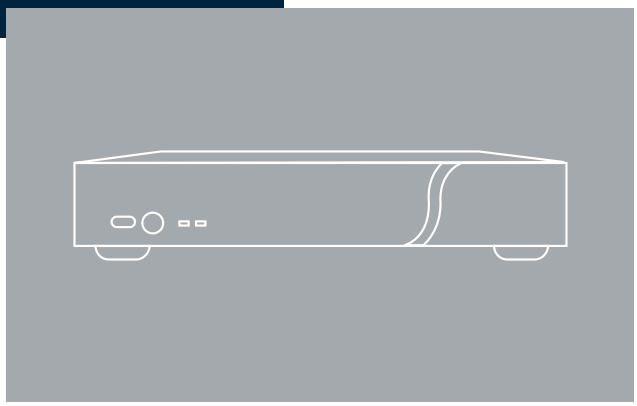


TABLE OF CONTENTS

Overview

No one can prevent all cybercrimes, but we go above and beyond to keep it from happening. In addition to standard industry security practices, Speco Technologies extends its efforts in cybersecurity by assessing, mitigating or neutralizing vulnerabilities or exploits identified throughout the product life cycle. Protecting our products is key in protecting our customers and reinforces Speco's place as your most trusted surveillance partner.

There are certain network-based protocols and services that may have potential weaknesses that could be exploited. While we have no control over these protocols, we do offer a network hardening guide to help your organization implement best practices and reduce the risks when using Speco Technologies products with these protocols and services. ***Download Hardening Guide Here***

We are committed to responding quickly to potential vulnerabilities and appreciate the opportunity to work with our customers, independent and corporate researchers, industry representatives and network/application security professionals, to identify and resolve potential vulnerabilities.

Vulnerability Action Process

1. Discovery: Vulnerabilities are uncovered through reports submitted from external entities or through our own internal testing.
2. Confirmation: Speco Technologies internal teams collaborate to identify and replicate the vulnerability and evaluate the risk level.
3. Mitigation: Once the cause of the vulnerability is determined, a fix is created for implementation into a new firmware release on a schedule determined by severity *(see Vulnerability Categories and Management below).*
4. Disclosure: Once the fix is ready, an announcement is sent out to our customer base for immediate application.

Reporting Suspected Vulnerabilities

Speco Technologies welcomes any accounts of suspected vulnerabilities or other security concerns with our products.

If you are an authorized installer on distributor, please contact our technical support department with your suspected vulnerability or other security concerns. You can reach technical support through our main number: ***1-800-645-5516*** or at ***techsupport@specotech.com***.

If you are an end user, please send an e-mail to ***orders@specotech.com*** with as much detail as you're able to provide. A technician will contact you and work with you to gather the necessary details to determine an appropriate course of action.

Vulnerability Categories and Management

Speco Technologies investigates and prioritizes reported vulnerabilities based on the severity of the exploit and communicates the vulnerability impact using the industry standard Common Vulnerability Scoring System (CVSS). A security advisory is typically only issued for vulnerabilities specific to Speco Technologies products. The priority for a vulnerability is as follows:

CVSS 7.0-8.9 (High) and 9.0 to 10.0 (Critical):
Speco Technologies places highest priority on vulnerabilities assigned a score in this range and sets a deadline of 3 weeks or sooner after the external disclosure to issue a patch.

CVSS 4.0-6.9 (Medium):
Speco Technologies sets a deadline of 1 to 3 months to issue a patch.

CVSS 0.1-3.9 (Low):
Speco Technologies sets a deadline of issuing a patch in an upcoming firmware revision.

Supported Products

Highest priority is placed on active products. Once a product is retired, we will address CVSS Critical vulnerabilities for 1 year. Information on active and retired products can be found at ***www.specotech.com.***

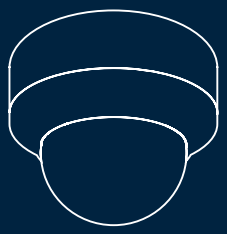
Security Advisories

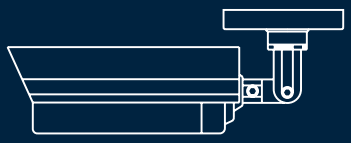
Speco Technologies will issue a security advisory to communicate information regarding vulnerabilities and security exposures. This advisory will contain pertinent information including applicability, impact and mitigation options. These advisories may address security issues that involve Speco Technologies both directly and indirectly.

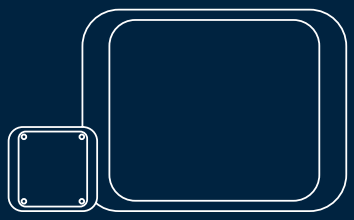
Vulnerability Disclosure Policy

As part of our best practice philosophy, Speco Technologies is committed to disclose information (at our discretion) providing details on the vulnerability in question, including the CVSS score. Our goal is to help customers understand their risks as well as clearly know what steps they can take to mitigate the vulnerability. We urge all customers to always keep their firmware as current as possible to take advantage of the latest fixes.

Verison V.1 | 07/12/22







About Speco

For over sixty years, Speco Technologies has been dedicated to providing the latest access control innovations in video surveillance and audio products. We have committed ourselves to providing affordable, dependable merchandise, delivering exceptional customer service, and offering extensive product training, technical and marketing support. We will continue to be an innovator in both the residential and commercial solutions and want our customers to grow with us and move forward.

www.specotech.com

follow us on social media