TECHNICAL NOTE

REFERENCE DOCUMENT

XSS Vulnerabilities and Security Releases for the AXIS 2100/2120

Created: 16 October 2007

Last updated: 9 November 2007

Rev: 1.0

TABLE OF CONTENTS

1Introduction

A security release, 2100-2_43—boa-sec-fixes.zip, is available for the AXIS 2100/2120 that will reduce the risk of two cross-site scripting (XSS) vulnerabilities.

Listed below are the vulnerabilities that are addressed with this security release, as well as the vulnerabilities that are not addressed by this security release. Currently, Axis does not plan another security or firmware release for the AXIS 2100/2120, but is working to produce a firmware release to reduce the risk of these other (XSS) vulnerabilities in other Axis video products.

2Vulnerabilities that have been addressed with the Security Release

The following two vulnerabilities are addressed with the 2100-2_43—boa-sec-fixes.zip security release:

- XSS on 404 error pages: cross-browser XSS phishing
- Persistent XSS on the logs viewing facility: stealing the `passwd` file

Please contact Support at www.axis.com for information about how to download and install this security release.

3Vulnerabilities that will be addressed in Future Firmware and Security Releases

Below is a list of vulnerabilities that Axis will address in a future firmware release for other Axis video products:

- Persistent XSS on the network settings page
- Persistent XSS on the video viewing page: replacing the video stream
- Persistent XSS on the video viewing facility: adding a backdoor account

Routinely check the support page for your Axis video products for information about firmware releases that contain the latest security updates.