Security Notification – Pelco Sarix Professional V1.2

27-Feb-2018 **(Updated 6-Apr-2018)**

Overview

Schneider Electric has become aware of vulnerabilities in the Pelco Sarix Pro 1 cameras.

Vulnerability Overview

The vulnerabilities identified include:

- Information disclosure
- Authentication Bypass
- XML external entity
- Command execution
- Arbitrary file download
- Arbitrary file delete
- Buffer overflow

Product(s) Affected

The products affected:

- Pelco Sarix Pro 1st generation with firmware versions prior to 3.29.67

Pelco Sarix Pro 2 (next generation) cameras are not affected.

Indoor Domes	Outdoor Domes (non-IR)	Outdoor Domes (IR)	Bullets
IMPS110-1	IMPS110-1E	IMPS110-1ER	IBPS110-1ER
IMP1110-1	IMP1110-1E	IMP1110-1ER	IBP1110-1ER
IMP219-1	IMP219-1E	IMP219-1ER	IBP219-1ER
IMP319-1	IMP319-1E	IMP319-1ER	IBP319-1ER
IMP519-1	IMP519-1E	IMP519-1ER	IBP519-1ER

Release notes link - https://www.pelco.com/search?documentUUID=e88d9bca-0062-4f85-8f41-65982d304c69&title=Sarix%20Professional%20--%20Firmware%20Release%20Notes%20v3.29.67#tab/documents

Vulnerability Details

The list of vulnerabilities identified are below:

1. Information Disclosure

Retrieving specially crafted URLs without authentication can reveal sensitive information to an attacker.

Overall CVSS Score: 5.3 (Medium)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID: CVE-2018-7227 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7227

2. Authentication Bypass

A vulnerability exists which could allow an unauthenticated, remote attacker to bypass authentication and get the administrator privileges.

Overall CVSS Score: 7.5 (High)

(CVSS V3 Vector):CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVE ID: CVE-2018-7228 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7228

3. Authentication Bypass

Due to hard coded credentials, an unauthenticated, remote attacker can bypass authentication and gain administrator privileges.

Overall CVSS Score: 7.5 (High)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

CVE ID: CVE-2018-7229 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7229

4. XML External Entity Vulnerability

A XML external entity (XXE) vulnerability exist in the import.cgi of the web interface.

Overall CVSS Score: 7.4 (High)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N

CVE ID: CVE-2018-7230 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7230**

5. Command Execution - 'system.opkg.remove'

Lack of validation of the shell meta characters with the value of 'system.opkg.remove' allows execution of commands.

Overall CVSS Score: 9.8 (Critical)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID: CVE-2018-7231 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7231**

6. Command Execution - 'network.ieee8021x.delete_certs'

Lack of validation of the shell meta characters with the value of 'network.ieee8021x.delete_certs' allows execution of commands.

Overall CVSS Score: **9.4 (Critical)**

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVE ID: CVE-2018-7232 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7232**

7. Command Execution - 'model_name' or 'mac_address'

Lack of validation of the shell meta characters with the values of 'model_name'or 'mac_address'and allows execution of the commands.

Overall CVSS Score: 9.4 (Critical)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVE ID: CVE-2018-7233 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7233**

8. Arbitrary File Download

Lack of validation of SSL certificate file allows arbitrary system file download.

Overall CVSS Score: 8.2 (High)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

CVE ID: CVE-2018-7234 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7234**

9. Command Execution - 'system.download.sd_file'

Lack of validate of the shell meta characters with the value of 'system.download.sd_file' allows execution of commands.

Overall CVSS Score:8.8 (High)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE ID: CVE-2018-7235 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7235**

10. Authentication Bypass

Lack of authentication for /login/bin/set_param could enable SSH service.

Overall CVSS Score: **8.1 (High)**

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N

CVE ID: CVE-2018-7236 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7236**

11. Arbitrary File Delete

Lack of validation of the /login/bin/set_param to the file name with the value of 'system.delete.sd_file' which could allow a remote attacker to delete arbitrary system file.

Overall CVSS Score: **9.4 (Critical)**

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

CVE ID: CVE-2018-7237 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7237

12. Buffer Overflow

A buffer overflow vulnerability exist in the web-based GUI of Sarix Pro that could allow an unauthenticated, remote attacker to execute arbitrary code.

Overall CVSS Score: **8.4 (High)**

(CVSS V3 Vector): CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVE ID: CVE-2018-7238 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7238

Mitigation

Firmware version 3.29.67 with the fix for these vulnerabilities is available for download here:

https://www.pelco.com/search#keyword/v3.29.67/tab/documents

Acknowledgements

Schneider Electric would like to thank the following for all their efforts related to identification and coordination of these vulnerabilities:

CVE-2018-7227	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7228	• Deng Yongkai of NSFOCUS Security Team • Melih Berk Eksioglu of Biznet Bilisim A.S. • Giri Veeraraghavan Veda of Gulf Business Machines
CVE-2018-7229	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7230	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7231	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7232	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7233	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7234	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7235	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7236	• Deng Yongkai of NSFOCUS Security Team • Gjoko Krstic of Zero Science Labs
CVE-2018-7237	• Deng Yongkai of NSFOCUS Security Team
CVE-2018-7238	• Deng Yongkai of NSFOCUS Security Team

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. WE RESERVE THE RIGHT TO UPDATE OR CHANGE THIS INFORMATION AT ANY TIME AND IN OUR SOLE DISCRETION.

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *27 February 2018*	Original Release
Version 1.1 *1 March 2018*	Page 6 - Acknowledgements updated
Version 1.2 *6 April 2018*	Page 1 - Sarix Pro 2 not affected

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.04.06 11:12:53 -04'00'