# Security Notification – Pelco Sarix Professional

24-Apr-2018

## Overview

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

## Vulnerability Overview

The vulnerabilities identified include:

- Buffer Overflow
- Authenticated password disclosure and privilege escalation
- Authenticated password disclosure

## Product(s) Affected

The products affected:

- Pelco Sarix Pro 1st generation with firmware versions prior to 3.29.69

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 |

Link to Release Notes – https://www.pelco.com/search?documentUUID=a6b0528a-3627-4dc9-b2ca-5a21c5faa9ad&title=Sarix%20Professional%20IBP219-ER%20-%20Firmware%20v3.29.69%20(zip)

## Vulnerability Details

The list of vulnerabilities identified are below:

**1. Buffer Overflow**
A buffer overflow vulnerability exist in cgi program "set".

**Overall CVSS Score: 7.2 (High)**

**(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-2018-7780

**2. Authenticated password disclosure and privilege escalation**

By sending a specially crafted request an authenticated user can view password in clear text and results in privilege escalation

**Overall CVSS Score: 7.7 (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-2018-7781

**3. Authenticated password disclosure**

Authenticated users can view passwords in clear text.

**Overall CVSS Score: 7.1 (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-2018-7782

## Mitigation

Firmware version 3.29.69 with the fix for these vulnerabilities is available for download here:

https://www.pelco.com/search#keyword/v3.29.69/tab/documents

## Acknowledgements

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

| | |
|---|---|
| Weapon x | CVE-2018-7780 |
| Giri Veeraraghavan Veda<br>(Gulf Business Machines) | CVE-2018-7781<br>CVE-2018-7782 |

## 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



**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**<br>*24 April 2018* | Original Release |

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: 2018.04.24 16:29:46 -04'00'