Schneider Electric Security Notification

Security Notification –
Pelco Sarix Enhanced and Spectra Enhanced

14 February 2019

Overview

Schneider Electric has become aware of multiple vulnerabilities in the first generation of Sarix Enhanced and Spectra Enhanced cameras.

Affected Product(s)

Pelco Sarix Enhanced 1st generation*.

Indoor Cameras
- IMES19-1I, IMES19-1S, IMES19-1P
- IME119-1I, IME119-1S, IME119-1P
- IME219-1I, IME219-1S, IME219-1P
- IME319-1I, IME319-1S, IME319-1P
- IME319-B1I, IME319-B1S, IME319-B1P
- IME3122-1I, IME3122-B1I, IME3122-1S, IME3122-B1S, IME3122-1P, IME3122-B1P

Environmental Cameras Mini Domes
- IMES19-1EI, IMES19-1ES, IMES19-1EP
- IME119-1EI, IME119-1ES, IME119-1EP
- IME219-1EI, IME219-1ES, IME219-1EP
- IME319-1EI, IME319-1ES, IME319-1EP
- IME3122-1EI, IME3122-1ES, IME3122-1EP

Vandal Resistant Mini Domes
- IMES19-1VI, IMES19-1VS, IMES19-1VP
- IME119-1VI, IME119-1VS, IME119-1VP
- IME219-1VI, IME219-1VS, IME219-1VP
- IME319-1VI, IME319-1VS, IME319-1VP
- IME3122-1VI, IME3122-1VS, IME3122-1VP

Box Cameras
- IXES1
- IXE11
- IXE21
- IXE31

*Note: next generation Pelco Sarix Enhanced cameras are not affected.

Spectra Enhanced PTZ
- D6220, D6220L
- D6230, D6230L

Vulnerability Details

CVE ID: **CVE-2018-7816**

7.6 | (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L
A Permissions, Privileges, and Access Control vulnerability exists in the web-based GUI of the 1st Gen Pelco Sarix Enhanced Camera that could allow a remote attacker to delete an arbitrary file .

CVE ID: **CVE-2018-7825**

8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
A Command Injection vulnerability exists in the web-based GUI of the 1st Gen Pelco Sarix Enhanced Camera that could allow a remote attacker to execute arbitrary commands .

CVE ID: **CVE-2018-7826**

8.8 | (High) | CVSS:3.0/ AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
A Command Injection vulnerability exists in the web-based GUI of the 1st Gen Pelco Sarix Enhanced Camera that could allow a remote attacker to execute arbitrary commands.

CVE ID: **CVE-2018-7827**

8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
A Cross-Site Scripting (XSS) vulnerability exists in the 1st Gen. Pelco Sarix Enhanced Camera and Spectra Enhanced PTZ Camera which a remote attacker can execute arbitrary HTML and script code in a user's browser session.

CVE ID: **CVE-2018-7828**

8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
A Cross-Site Request Forgery (CSRF) vulnerability exists in the 1st Gen. Pelco Sarix Enhanced Camera and Spectra Enhanced PTZ Camera when an authenticated user clicks a specially crafted malicious link while logged into the camera.

Schneider Electric Security Notification

CVE ID: **CVE-2018-7829**

8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
An Improper Neutralization of Special Elements in Query vulnerability exists in the 1st Gen. Pelco Sarix Enhanced Camera and Spectra Enhanced PTZ Camera which allows an attacker to execute arbitrary system commands.

Remediation

These vulnerabilities are fixed with the release of firmware version 2.2.3.0 for Sarix Enhanced and with 2.11 and higher on Spectra Enhanced.
A fix for these vulnerabilities on the first generation Sarix Enhanced is available for download below:
1st Gen Sarix Enhanced (Dome style)
https://www.pelco.com/search#Asset%20Type!Firmware!11002,Cameras!Sarix%20IME%20Series%20Environmental!3016172,Cameras!Sarix%20IME%20Series%20Indoor%20Mini!3016169,Cameras!Sarix%20IME%20Vandal%20Mini!3016171/tab/documents
1st Gen Sarix Enhanced (Box style)
https://www.pelco.com/search#Cameras!Sarix%20IXE!3016155/tab/documents

A fix for these vulnerabilities on the Spectra Enhanced is available for download below:
Spectra Enhanced
https://www.pelco.com/ptz-ip-cameras/spectra-enhanced-hd-ip-dome-camera#downloads

These first generation Sarix Enhanced cameras are directly replaced by the Sarix Enhanced Next Generation Series of cameras, which have not been affected by these vulnerabilities, and can be used with confidence.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.

- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric would like to recognize the following researcher(s) for all their efforts related to identification and coordination of this vulnerability:

CVE	Researcher(s) Name
CVE-2018-7816, CVE-2018-7825, CVE-2018-7826	Deng Yongkai (NSFOCUS)
CVE-2018-7827	Gjoko Krstic (Zero Science)

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
If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

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. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS 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 *14 Feb 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.02.13 15:56:06 -05'00'