Security Notification – Pelco VideoXpert Enterprise

05-Dec-2017

Overview

Schneider Electric has become aware of three vulnerabilities in the Pelco VideoXpert Enterprise.

Vulnerability Overview

The vulnerabilities identified are:

- Exposure of Sensitive Information, Security Bypass
- Exposure of System Information, Exposure of Sensitive Information
- Privilege Escalation

Product(s) Affected

The product(s) affected:

- Pelco VideoXpert Enterprise, all versions prior to V2.1

Vulnerability Details

By sniffing communications, an unauthorized person can execute a directory traversal attack resulting in authentication bypass or session hijack.

Overall CVSS Score: 6.9 (Medium)

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

CVE ID: CVE-2017-9964 **https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-9964**

Using a directory traversal attack, an unauthorized person can view web server files.

Overall CVSS Score: 5.8 (Medium)

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

CVE ID: CVE-2017-9965 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-9965

By replacing certain files, an unauthorized user can obtain system privileges and the inserted code would execute at an elevated privilege level.

Overall CVSS Score: 7.1 (High)

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

CVE ID: CVE-2017-9966 https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-9966

Mitigation

A firmware with the fix, VideoXpert v2.1, for these vulnerabilities are available for download:

https://www.pelco.com/search?documentUUID=478b93c1-d908-4438-867f-7bcf849b28a8&title=VideoXpert%20Core%20Software%20v2.1

Acknowledgements

Schneider Electric would like to thank Gjoko Krstic for the effort related to identification of this vulnerability.

For More Information

This document is intended to help provide an overview of the identified vulnerability 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 on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Revision Control:

Version 1 *05 December 2017*	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: 2017.12.04 14:22:36 -05'00'