SIVMS®

Announcement for the release of a security update

PKE

A-1100 Wien, Computerstraße 6
Telefon: +43 50150 0
Telefax: +43 50150 1042
E-Mail: systems@pke.at

Dokumentversion 1.1
2021-04-06

TABLE OF CONTENTS

1 New Video Management and Control Center Server Update available

The product name SiNVR has been replaced by SiVMS, DiViCro and Zelaris.

In this article we would like to inform you that we offer the new version 5 for our video management application SiVMS (until version 3 also known and available as DiViCro, Zelaris and SiNVR). Likewise for the application Control Center Server (CCS) the new version 1.5.0 is available. Both versions include, among other new features, significant security optimizations and fix the following security vulnerabilities of the CVE database (https://cve.mitre.org):

1.1 SiVMS (Version 5.0.0)

- A security optimization has been implemented that prevents unauthorized HTTP access to the SiVMS video server (CVE-2019-18339).
- A security optimization has been implemented to prevent unauthorized access to port 5410 (CVE-2019-19297).
- A security enhancement has been implemented to prevent credentials of authorized users from appearing in plain text within the SiVMS system log (CVE-2019-19291).
- A security optimization has been implemented to prevent unauthorized FTP access (CVE-2019-19296).

1.2 Control Center Server (CCS Version 1.5.0)

- A security fix was implemented that prevents returning the file path within the XML interface (CVE-2019-18338).
- A security optimization has been implemented to prevent user data from being read (CVE-2019-18337).
- A security enhancement has been implemented to prevent the CCS database from being tampered with (CVE-2019-19292).
- Access to the directory service via S-FTP now requires a user and password (CVE-2019-18341).
- Access to the directory service via S-FTP has been revised (CVE-2019-18342).

  Now vaild:

  - S-FTP accesses are now only allowed in the SFTP_ROOT directory
  - Write permissions are only available in the import folders
  - Read permissions are now only available in all SFTP_ROOT folders
  - Only CSV files may be written

- Now FTP service passwords are encrypted in the communication log (CVE-2019-19291).
- A security optimization has been made, which prevents the so-called cross-site scripting (CVE-2019-19294)
- Furthermore, the ability to gain higher user group privileges via cross-site scripting was disabled CVE-2019-19293).

- Passwords are no longer transferred from CCS to the web client (CVE-2019-13947).
- The 'DOWNLOAD' section of the CCS is now protected from unauthorized access (CVE-2019-19290).
- By default, access to the web interface is now exclusively enabled for the local IP address. The following INI entry defines the IP address to which the web interface is bound:

  [WEBSERVICE]

  IP=127.0.0.1
- Now access (login attempts, failed logins) initiated through the CCS interface port (5444) and SiNEO interface port (5440) is logged within the system log (ControlCenterServer.LOG) (CVE-2019-19295).