SIVMS®

Bekanntgabe zur Veröffentlichung eines Sicherheitsupdates

PKE

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

Dokumentversion 1.0
2021-02-26

INHALTSVERZEICHNIS

1 Neues Videomanagement- und Control Center Server Update verfügbar

Der Produktname SiNVR wurde durch SiVMS, DiViCro und Zelaris abgelöst.

In diesem Artikel möchten wie Sie darüber informieren, dass wir für unsere Videomanagementanwendung SiVMS (bis Version 3 auch bekannt und erhältlich gewesen als DiViCro, Zelaris und SiNVR) die neue Version 5 anbieten. Ebenso steht für die Applikation Control Center Server (CCS) die neue Version 1.5.0 zur Verfügung. Beide Versionen beinhalten neben anderen neuen Leistungsmerkmalen auch signifikante Sicherheitsoptimierungen und beheben folgende Sicherheitslücken der CVE-Datenbank (https://cve.mitre.org):

1.1 SiVMS (Version 5.0.0)

- Es wurde eine Sicherheitsoptimierung implementiert, welche unberechtigte HTTP-Zugriffe auf den SiVMS-Videoserver verhindert (CVE-2019-18339).
- Es wurde eine Sicherheitsoptimierung implementiert, die unberechtigte Zugriffe auf Port 5410 verhindert (CVE-2019-19297).
- Es wurde eine Sicherheitsoptimierung implementiert, die verhindert, dass Zugangsdaten berechtigter Anwender innerhalb des SiVMS Systemlogbuchs in Klartext erscheinen (CVE-2019-19291).
- Es wurde eine Sicherheitsoptimierung implementiert, die unberechtigte FTP-Zugriffe verhindert (CVE-2019-19296).

1.2 Control Center Server (CCS Version 1.5.0)

- Es wurde eine Sicherheitsoptimierung implementiert, welche verhindert, den Dateipfad innerhalb der XML-Schnittstelle zurückzugeben (CVE-2019-18338).
- Es wurde eine Sicherheitsoptimierung implementiert, die verhindert, dass Benutzerdaten ausgelesen werden können (CVE-2019-18337).
- Es wurde eine Sicherheitsoptimierung implementiert, die verhindert, dass die CCS-Datenbank manipuliert werden kann (CVE-2019-19292).
- Der Zugriff auf den Verzeichnisdienst via S-FTP erfordert nunmehr die Angabe eines Benutzers und eines Passworts (CVE-2019-18341).
- Der Zugriff auf den Verzeichnisdienst mittels S-FTP wurde überarbeitet (CVE-2019-18342).

  Nunmehr gilt:

  - S-FTP-Zugriffe sind nur noch im SFTP_ROOT Verzeichnis erlaubt
  - Schreibberechtigungen sind nur in den Import Ordnern vorhanden
  - Leseberechtigungen sind nur noch in allen SFTP_ROOT Ordnern vorhanden
  - Es dürfen lediglich CSV-Dateien geschrieben werden

- Nunmehr werden Passwörter des FTP-Dienstes im Kommunikationslogbuch verschlüsselt (CVE-2019-19291).
- Es wurde eine Sicherheitsoptimierung vorgenommen, welche das so genannte Cross-Site Scripting unterbindet (CVE-2019-19294).

- Ferner wurde die Möglichkeit unterbunden, per Cross-Site Scripting höhere Benutzergruppenrechte zu erlangen CVE-2019-19293).
- Passwörter werden ab sofort nicht mehr vom CCS zum Webclient übertragen (CVE-2019-13947).
- Der 'DOWNLOAD'-Abschnitt des CCS ist nun vor unbefugtem Zugriff geschützt (CVE-2019-19290).
- Standardmäßig ist nunmehr der Zugriff auf das Web-Interface ausschließlich für die lokale IP-Adresse freigegeben. Über folgenden INI-Eintrag wird definiert auf welche IP-Adresse da Web-Interface gebunden wird:

  [WEBSERVICE]

  IP=127.0.0.1
- Nunmehr wird der Zugriff (Loginversuche, fehlgeschlagene Logins), die über den CCS Interface-Port (5444) und den SiNEO-Interface-Port (5440) initiiert werden, innerhalb des Systemlogbuchs (ControlCenterServer.LOG) protokolliert (CVE-2019-19295).