Security Bulletin

CVE-2020-25694, 25695, 25696

Summary

First published: October 31, 2023

Description	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24.
Affected Products	enteliSYNC
Recommended Action	Follow the enteliWEB Network Hardening Guide
CVSS v3.0 Base Score	7.8 High
CVE ID	CVE-2020-25694, CVE-2020-25695, CVE-2020-25696

Description

A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

Security Bulletin

Recommended Action

It is strongly recommend having an IT-managed firewall on the overall building network.

The enteliWEB Network Hardening Guide provides guidance used in planning and implementing security best practices in an enteliWEB installation but also applies to the enteliSYNC application. enteliWEB can be made more secure by configuring the following areas:

- Passwords
- Users and Groups Permissions Management
- Authentication
- Platform Management

Delta Controls is planning a release update to enteliSYNC April 2024. This application update will include an update to PostgreSQL version 15

17850 56 Ave Surrey BC Canada V3C 1C7 | Tel: 604.574.9444 | deltacontrols.com