REL-2022-02-09 User information disclosure with device-specific access

Overview

In the StrideLinx Cloud, users are assigned to one or multiple company-wide roles, and one or multiple device-specific roles, to finely tune what a user has access to. Due to a bug in the permissions-module, under specific circumstances, it was possible to view basic user information of other users even when you did not have “Manage Users” permissions.

Impact

A user with a company-wide role, without “Manage Users” permissions, could see other users in their company that had a device-specific role.It was not possible to interact, edit, or delete these users. Only basic information (username, email-address and assigned roles) was disclosed. No users of other companies were visible.

Product updates

API server v0.1.86.post1 was released on 09/02/2022, which tightens the code authorising access to users.

Recommendations

API releases are deployed automatically. No further action is required.

Additional information

-