CloudAware

Responsible Disclosure Document

Vulnerability type:	Authentication bypass for API
Vendor of the product:	Paxton
Product affected:	Paxton Net2 (version < 6.07.14023.5015 (SR4))
Date:	Oct 20 2024

Impact:	Exposure of PII, administration of users
Affected components:	Paxton Net2 software
Attack vector:	(Trivially) generate a license file to enable access to the API. Remote access to the computer running Paxton Net2 is sufficient to exploit.

Description:
Paxton Net2 software offers an API. This API offers the user access to sensitive data such as access logs and user data.[2]
In order to enable the API a licensefile is needed. The licensefile is trivial to generate as demonstrated in POC in ref [1]. License files can be generated while signature checks in the Net2 software were not functional.

Discoverer:	Jeroen Hermans j.hermans[at]cloudaware.eu Emiel van Berlo emiel[at]danego.nl
References:	[1] https://github.com/gitaware/poc_exploit_paxton_license [2] https://www.paxton-access.com/integrating-with-paxton/how-to-integrate-with-net2/integration-capability-matrix/