CloudAware

Advisory - CVE-2024-55447

Title: Potential PII leak and incorrect access control in Paxton Net2 software
Summary: Insecure backend database in the Paxton Net2 software. Possible leaking of PII incorrect access control.
Access cards can be cloned without physical access to the original card.
Audit log integrity compromised.
No physical access to computer running Paxton Net2 is required.
Exploit A working exploit is available on request
Date: 10-02-2025
Impact: Escalation of Privileges & Information Disclosure
Product: Paxton Net2 (all current versions)

Solution: As the vendor has not acknowledged the vulnerability there is no effective remediation for this vulnerability. The most effective measure at this moment is closely monitoring who has local access to the machine running the Net2 software.

Mitigation: There is no known effective mitigation. Limiting who has local access to the machine running the Net2 software seems the most effective measure.

Detailed description:
By exploiting MSSQL single user mode it is possible to gain administrator rights to the Net2 database. In this database plaintext PIN codes for building entrance can be found and changed. It is also possible to add users to the system and enable/disable users in the system. By reading tables in the MSSQL table PII is leaked.
Apart from the PII in plaintext in the database, card data is also stored unencrypted in the database. Using the data in the database cards can be cloned without having the original card if a Mifare or multi-protocol reader is used for building entrance.

The above vulnerabilities are also relevant for the integrity of the audit logs in Paxton Net2 software. These audit logs should never be used as forensic data. Not only is it possible cards are cloned, but audit log data can be manipulated directly in the database tables.

In order to gain access local access to the computer running Net2 is necessary, but this can also be over a network using e.g. Anydesk which makes physical access not necessary.

The vendor has not acknowledged the vulnerability after contact. There is no fix planned.

Weblinks:

- https://github.com/gitaware/CVE/tree/main/CVE-2024-55447
- https://seclists.org/fulldisclosure/2024/Dec/0
- exploit github available to help with mitigation

History: nov 12 2024: Requested latest Net2 software from Paxton
nov 26, 2024: Obtained latest Net2 software from other source than manufacturer
nov 26, 2024: Informed Paxton about vulnerability
nov 27, 2024: Release of exploit code
dec 2, 2024: Refused CVE reservation by Paxton & request of CVE reservation directly at Mitre
feb 10, 2025: CVE Assigned via Mitre

Credit: Jeroen Hermans j.hermans[at]cloudaware.eu
Emiel van Berlo emiel[at]danego.nl