CloudAware

Advisory - CVE-2023-43870

Title: Leaked private key of installed root certificate
Summary: Paxton Net2 software silently installs a root certificate in the OS trust store. The private key of this root certificate is leaked so a MITM attack is prossible.
Date: 19-12-2023
Impact: information disclosure
Product: Paxton Net2 (<v6.07 SR1)

Solution: 1) Upgrade Paxton Net2 software to version v6.07 SR1 or newer
2) Evaluate the trust store of the operating system as an unsecure trusted root certificate is installed by the Net2 software. Remove the unsecure certificate.

Mitigation: If an upgrade is not an option, ensure the unsecure root certificate is removed from the trust store and use a local self-signed certificate for the web interface of the Net2 software.

Detailed description:
When installing the Net2 software a root certificate is silently installed into the trust store of the operating system. The private key of this trusted root certificate has leaked. This leads to a potential MITM attack on computers where the Net2 software has been installed.
No physical access to the computer running Net2 is necessary as the attacker can run a webservice using a TLS certificate signed by the trusted Paxton root certificate.

The vendor has fixed this in version 6.07 SR1 of the Net2 software.

Weblinks:
- https://github.com/gitaware/CVE/tree/main/CVE-2023-43870
- https://cloudaware.eu/blog/paxton_tls/
- https://nvd.nist.gov/vuln/detail/CVE-2023-43870

History: 20-4-2023: Initial contact with Paxton for resp. discl.
28-4-2023: Paxton confirms vulnerability
19-9-2023: Another customer contacts Paxton for same vulnerability
2-10-2023: Vulnerability fixed in v 6.07 SR1
19-12-2023: publication of CVE

Credit: Jeroen Hermans j.hermans[at]cloudaware.eu

Bezuidenhoutseweg 98, NL-2594AZ Den Haag (NL)
T.: +31 (0)85 782 8878 E.: info@cloudaware.eu
KvK: 75426153