



Piciorgros TMO-100: Unautorisierter Zugriff auf Log-Daten

Georg Lukas, rt-solutions.de GmbH, 2025-02-26, geändert 2025-04-11

Klassifikation

- [CWE-200: Exposure of Sensitive Information to an Unauthorized Actor](#)
- CVSS 4.0 Score: 5.3 / Medium
[CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N](#)
- CVSS 3.1 Score: 4.3 / Medium [CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N](#)

Betroffene Systeme

- Piciorgros TMO-100 V3/V4 mit Software-Version unter 4.20 (entdeckt bei V3.72)

Zusammenfassung

Das Piciorgros TMO-100 ist ein Datenmodem für TETRA-Funknetze. Es verfügt über einen nicht dokumentierten Zugang zum System-Log, der ohne Authentifizierung über den TCP-Port 51986 auf der LAN-Schnittstelle bereitgestellt wird. Darüber kann ein Angreifer mit Zugriff zum LAN-Netzwerk einige Betriebsparameter des Modems einsehen, um so ggfs. weitere Angriffe zu planen. Ab Software-Version 4.20 wird der Logger-Zugriff nur noch für ein 15-minütiges Zeitfenster nach einem Web-Login aktiviert, um Angriffe während des Normalbetriebs zu verhindern.

Details

Bei einem im Kundenauftrag durchgeführten Penetrationstest war ein Piciorgros TMO-100-Datenmodem Teil des Prüfumfangs. In der Dokumentation wird für Support-Anfragen beim Hersteller das sog. „IPLog“ beschrieben, welches mit der Software [IP Logger](#) abgerufen werden kann. Technisch erfolgt der Zugriff dabei über TCP-Port 51968 auf der LAN-Schnittstelle, auf dem das Modem ohne eine Authentifizierung die aktuellen System-Protokoll-Daten und einen Live-Datenstrom liefert:

```
$ telnet 192.168.0.199 51968
Trying 192.168.0.199...
Connected to 192.168.0.199.
Escape character is '^]'.

[FFFF] | 13.02.25 10:43:25 02:37:37.43 | **** Piciorgros TMO-100 V3.72 (HW-
Rev. 3) Build 1819* Release (Apr 7 2021, 10:35:03) - Logging started ****
[FFFE] | 13.02.25 10:43:25 02:37:37.43 | Serial number: [REDACTED] Options: 8001
Set24: 0080 Set25: 0001
[FFFE] | 13.02.25 10:43:25 02:37:37.43 | TETRA core SW versions: Stack:0454,
DSP:0456, MMI:F444
[F020] | 13.02.25 10:43:38 02:37:51.16 | TETRA CREG state change: 1 -> 99:1:0
...
[E000] | 13.02.25 10:44:34 02:38:46.63 | TETRA registration information:
1:0:0.
[F020] | 13.02.25 10:44:41 02:38:53.97 | PPP: Is up.
[E000] | 13.02.25 10:44:41 02:38:53.98 | PPP link is up in try 1. Own IP:
10.14.42.31
...
```



Aus dem Log ergibt sich die IP-Adresse des Modems im TETRA-Netz, die verwendet werden kann, um Angriffe auf andere Geräte im TETRA-Datennetz auszuführen.

Auswirkungen

Ein Angreifer, der LAN-Zugriff zu einem TMO-100-Modem hat, kann die eingesetzte Hardware- und Software-Version sowie die IP-Adresse im TETRA-Datennetz ermitteln, und so das Modem nutzen, um benachbarte IP-Addressbereiche zu scannen.

Mitigation für Betreiber

Die Modems sollten mindestens auf Software-Version 4.20 aktualisiert werden, um die Angreifbarkeit einzuschränken.

Empfehlungen für den Hersteller

Der Zugriff sollte analog zum Web-Interface authentifiziert und ggfs. TLS-verschlüsselt werden. Denkbar wäre eine Umsetzung mittels Web-Sockets oder anderer APIs als Teil der Web-UI.

Timeline

- 2025-02-13 Entdeckung der Schwachstelle
- 2025-02-27 Meldung an den Hersteller
- 2025-03-06 Bestätigung der Schwachstelle durch den Hersteller
- 2025-03-11 Veröffentlichung der Software-Version V4.20 durch den Hersteller
- 2025-08-14 Veröffentlichung der Schwachstelle im Rahmen von Responsible Disclosure

Kontakt

Dr.-Ing. Georg Lukas <lukas@rt-solutions.de>

rt-solutions.de GmbH - Oberländer Ufer 190a - 50968 Köln - (+49)221 93724 0