rt-solutions.de
experts you can trust.

Piciorgros TMO-100: Unautorisierte Konfigurationsänderung über TFTP (CVE-2025-29617)

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

Klassifikation

- CWE-306: Missing Authentication for Critical Function
- CWE-940: Improper Verification of Source of a Communication Channel
- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- CVSS 4.0 Score: 8.4 / High
  CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:L/SI:N/SA:H
- CVSS 3.1 Score: 8.3 / High
  CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

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 abschaltbaren TFTP-Zugang, über den sich die interne Konfiguration ohne Authentifizierung auslesen und schreiben lässt. Der TFTP-Zugriff ist sowohl über LAN als auch über TETRA möglich, so dass ein Angreifer, der sich Zugriff auf eines dieser Netzwerke verschafft hat, die Konfiguration aller Modems im selben TETRA-Datennetz verändern kann. Damit kann der Angreifer per Port-Forwarding Zugriff auf dahinterliegende Systeme freischalten, oder die Einwahldaten der Modems löschen, um so z.B. KRITIS-Anlagen zu sabotieren. Ab Software-Version 4.20 wird der TFTP-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. Aus der Dokumentation und aus durchgeführten Portscans ergab sich, dass ein TFTP-Server (UDP-Port 69) zum Hochladen der Firmware, für den Zugriff auf die Konfiguration („config.tmo"), Voice Alarms („voicealarms.tmo") und eine weitere Datei („plog.tmo") aktiv ist. Der Zugriff erfolgt über die vom Hersteller angebotene Software IP Loader oder mit einem TFTP-Client:

```
$ atftp 192.168.0.199
tftp> get config.tmo
tftp>
$ ls -al config.tmo
-rw-rw-r-- 1 pentest pentest 157184 Feb 21 16:13 config.tmo
```

Dieser Zugriff ist sowohl über LAN als auch über das TETRA-Datennetz möglich. Die abgerufene Datei „config.tmo" enthält sämtliche Konfigurationsparameter des Modems in einem binären Format, jedoch kein TETRA-Schlüsselmaterial. Enthalten sind sensitive Daten wie:

- TETRA-Parameter (SSI, TMCC, TMNC)
- PPP-Login-Daten (Nutzer und Passwort im Klartext)
- LAN-Konfiguration (IP-Adresse, Netzwerkmaske, Gateway)
- Port-Forwarding-Konfiguration (Global Forwarding / Ports und IPs)

Auszüge aus der Konfigurationsdatei mit markierten Feldern:

- Modem-LAN-IP: **c0a800c7** = 192.168.0.199
- Netzwerk-Maske: **fffff000** = 255.255.240.0
- Standard-Gateway: **c0a80001** = 192.168.0.1

```
000000a0: 0000 0000 0000 0000 0000 003f 0000 c0a8  ...........?....
000000b0: 00c7 ffff f000 c0a8 0001 0050 1273 0045  ...........P.s.E
```

PPP-Zugangsdaten: „TMO“ / „TMO“, Kennung des Modems: „TMO-100“

```
000002a0: 0000 0000 0000 0000 0000 0000 544d 4f00  ............TMO.
000002b0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
000002c0: 544d 4f00 0000 0000 0000 0000 0000 0000  TMO.............
000002d0: 0000 0000 544d 4f2d 3130 3000 0000 0000  ....TMO-100.....
```

Dieser Zugriff erlaubt auch das Herunterladen, Modifizieren und Hochladen der Konfigurationsdatei, um so weitergehende Zugriffe zu erhalten. Dazu muss entweder das Format vollständig reverse-engineered werden, oder man benötigt ein zweites Modem, auf dem man die Konfiguration einspielen und über das Web-Interface nach Bedarf anpassen kann.

Auswirkungen

Ein Angreifer, der LAN-Zugriff zu einem TMO-100-Modem oder zum TETRA-Datennetz hat, kann die Konfiguration sämtlicher an das Datennetz angeschlossener Modems abrufen und manipulieren, ohne dafür Zugangsdaten kennen zu müssen. Durch Veränderung der Port-Forwaring-Konfiguration kann er so Zugriff auf die hinter anderen Datenmodems angeschlossenen Geräte erhalten, und durch Verändern der TETRA-Parameter das Modem offline nehmen, sodass ein Service-Techniker vor Ort kommen muss.

Mitigation für Betreiber

Die Modems sollten mindestens auf Software-Version 4.20 aktualisiert werden, um die Angreifbarkeit einzuschränken. Der TFTP-Port kann im Web-Interface auf einen Non-Standard-Wert geändert werden, um eine Entdeckung durch Angreifer weiter zu erschweren. Soweit möglich, sollte der TFTP-Zugriff durch externe Firewalls unterbunden werden.

Timeline

- 2025-02-21 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