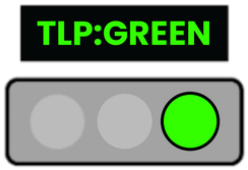
Catena del freddo e sistemi OT/IoT connessi
Comunicato di sicurezza

05/11/2026



AVVERTENZE

ARIA S.P.A., nell'erogare al meglio questo servizio, si avvale di propri fornitori e di fonti pubbliche disponibili in Rete, individuati e selezionati tra i più autorevoli organismi di sicurezza, aziende specializzate e fornitori di tecnologie, al fine di garantire alla comunità di riferimento – con la massima accuratezza, affidabilità e tempestività possibile – le informazioni utili per la prevenzione e la gestione degli incidenti di sicurezza informatica. Non è consentito far uso di queste informazioni per finalità differenti da quelle sopra indicate. La presenza di rinvii operati mediante tecniche di ipertesto (link) non costituisce una raccomandazione di ARIA S.P.A. verso il soggetto richiamato, ma unicamente uno strumento per facilitare il rapido recupero di informazioni utili.

Invito a verificare con urgenza

A seguito del comunicato dell'Agenzia per la cybersicurezza nazionale (ACN) del 4 novembre 2026, il Cyber Security Operation Center (CSOC) di ARIA S.p.A. invita gli Enti della constituency di Regione Lombardia che impiegano tecnologie per il mantenimento della catena del freddo, nonché sistemi di telecontrollo e supervisione degli impianti, a prendere in carico **con la massima urgenza** le attività di verifica e mitigazione raccomandate dall'Agenzia.

Particolare attenzione deve essere rivolta ai sistemi da cui dipendono **la conservazione di emocomponenti, farmaci, vaccini, campioni biologici e alimenti** e il condizionamento di ambienti critici. L'esposizione non adeguatamente protetta di questi sistemi può consentire accessi non autorizzati, l'alterazione dei parametri operativi e delle soglie di allarme e la compromissione delle funzionalità di notifica, con possibili ripercussioni sulla continuità dei servizi e sulla salute delle persone.

Il richiamo riguarda, più in generale, **tutti i dispositivi connessi e le relative interfacce di amministrazione e monitoraggio** a supporto degli impianti: building automation e climatizzazione, reti idriche, sistemi di produzione e distribuzione dell'energia, videosorveglianza e controllo accessi, comprese le piattaforme di gestione centralizzata, attraverso le quali gli effetti di un incidente possono estendersi a più sedi.

Si invita ciascun Ente a **verificare il proprio perimetro**, a partire dai sistemi a supporto di beni e servizi sanitari, con priorità alla **rimozione dell'esposizione diretta su Internet** delle interfacce amministrative e di controllo, alla **verifica dell'integrità dei parametri operativi** e del **corretto funzionamento dei sistemi di allarme**. È inoltre necessario verificare gli account abilitati all'accesso, la robustezza delle credenziali, lo stato di aggiornamento dei dispositivi e la protezione degli accessi remoti, che devono avvenire solo tramite canali autorizzati dall'Ente e con autenticazione a più fattori.

Poiché molti di questi sistemi sono installati, gestiti o assistiti da remoto da terzi, **le verifiche devono coinvolgere anche i fornitori**. Si chiede agli Enti di trasmettere il presente comunicato a produttori, installatori, manutentori e gestori di piattaforme di telemonitoraggio, chiedendo loro di **verificare a loro volta** i sistemi installati o gestiti e le proprie piattaforme, di estendere le verifiche ai propri subfornitori e di comunicare all'Ente gli esiti e le eventuali criticità.

Come buona pratica si consiglia di mantenere un inventario aggiornato dei dispositivi connessi, di separare i sistemi di controllo dalla rete aziendale e da Internet, di monitorare con continuità gli accessi e le modifiche alle configurazioni.

In presenza di anomalie o di elementi che possano indicare una potenziale compromissione si raccomanda di isolare il sistema dalla rete senza interromperne il funzionamento locale, mettere in sicurezza i beni conservati, preservare le evidenze, attivare le procedure di gestione degli incidenti e **darne tempestiva segnalazione al CSOC** (cybersoc@ariaspa.it), valutando gli eventuali obblighi di notifica a CSIRT Italia.

Indicazioni operative per le verifiche

Sistemi da considerare. Rientrano nelle verifiche frigoemoteche e congelatori dei Servizi trasfusionali, frigoriferi delle farmacie, celle per vaccini, congelatori di laboratori e biobanche, sistemi di monitoraggio delle temperature, cucine e mense di ospedali, building automation e climatizzazione di sale operatorie e terapie intensive, compresi i sistemi gestiti da terzi e le piattaforme cloud dei produttori.

Esposizione su Internet. La verifica va condotta sugli indirizzi IP pubblici dell'Ente, comprese le connessioni predisposte da terzi per manutenzione e teleassistenza. Come indicato da CSIRT Italia nel bollettino BL01/250626/CSIRT-ITA, riportato in evidenza il 4 novembre 2026, vanno ricercati in particolare le interfacce web di configurazione e controllo dei dispositivi (HTTP/HTTPS), i servizi di accesso remoto (Telnet, SSH, RDP, VNC), i protocolli industriali e di building automation privi di sicurezza intrinseca (Modbus, DNP3, BACnet), i flussi delle telecamere IP (RTSP) e i protocolli IoT e di gestione come MQTT, CoAP, SNMP, FTP e UPnP. Dove non possono essere eliminati, questi servizi vanno resi accessibili solo tramite VPN o da indirizzi autorizzati, preferendo le versioni cifrate dei protocolli, come SNMPv3, SFTP o BACnet/SC.

Parametri e allarmi. Soglie e ritardi di allarme e destinatari delle notifiche vanno confrontati con i valori attesi, salvando le evidenze prima di ripristinare eventuali difformità. Tutti i canali di notifica vanno provati, verificando la presenza di un allarme o di un registratore di temperatura indipendente dalla piattaforma connessa. Per emocomponenti, vaccini e farmaci termolabili è opportuno intensificare il controllo manuale delle temperature fino al completamento delle verifiche ed esportare eventuali log disponibili prima che vengano sovrascritti.

Accessi remoti e account. L'accesso remoto deve passare da un unico punto gestito dall'Ente, con autenticazione a più fattori e sessioni abilitate su richiesta e registrate. Eventuali modem, tunnel e strumenti di controllo remoto installati autonomamente da terzi dovranno essere dismessi. Gli account devono essere nominativi e limitati al necessario, rimuovendo quelli di personale e tecnici non più incaricati. I dispositivi non più supportati dai produttori vanno isolati e avviati a una dismissione controllata, con migrazione verso soluzioni supportate.

Verifiche richieste ai fornitori. I fornitori devono confermare che i sistemi installati o gestiti non sono esposti su Internet e sono raggiungibili tramite canali autorizzati e conosciuti dall'Ente e che non sono in uso credenziali predefinite o condivise tra clienti diversi. I gestori di piattaforme centralizzate devono inoltre verificare la protezione con autenticazione a più fattori degli account amministrativi, la segregazione tra clienti ed il monitoraggio degli accessi.

Segnali di possibile compromissione. Meritano attenzione le modifiche di soglie di allarme non pianificate, la disattivazione delle notifiche o l'assenza di quelle di routine, valori di temperatura incoerenti con gli strumenti indipendenti, accessi da indirizzi IP esteri o non riconducibili a fornitori autorizzati o fuori dagli orari concordati, nuovi account o cambi di password non richiesti, riavvii e modifiche di configurazione non pianificati.

Contenuto della segnalazione. Nella segnalazione al CSOC è utile indicare Ente e sito, sistema coinvolto (produttore e modello), data e ora di rilevazione, parametri alterati, indirizzi IP osservati, eventuale fornitore coinvolto e azioni già intraprese.

Riferimenti

ACN, comunicato del 04/11/2026: Sicurezza dei sistemi a supporto della catena del freddo – richiamo urgente alle misure di verifica e mitigazione

ACN: Misure urgenti di verifica e mitigazione per operatori della distribuzione alimentare e della filiera del freddo

CSIRT Italia, bollettino BL01/250626/CSIRT-ITA: Dispositivi IoT e servizi di accesso remoto connessi ad Internet: rischi e mitigazioni