
# Elementi essenziali e gestione della sicurezza informatica (settore energetico)

# CSP001

Argomento 2/10: Conoscenze di base e tassonomia della sicurezza informatica nel settore energetico.

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

# Cybersecurity nel settore energetico


## Vulnerabilità

- Valutazione della vulnerabilità: processo sistematico di identificazione, quantificazione e prioritizzazione delle vulnerabilità in un sistema, una rete o un'infrastruttura.
- Scopo: identificare i punti deboli, misurare il potenziale impatto e fornire indicazioni per la mitigazione.
- Metodologia: scansione, test manuali e analisi.
- Tipi: rete, applicazione, infrastruttura.
- Risultato: rapporto sulle vulnerabilità, valutazione dei rischi.
- Vantaggi: sicurezza proattiva, conformità, gestione dei rischi.
- Sfide: falsi positivi, uso intensivo di risorse, minacce in continua evoluzione.
- Best practice: valutazioni regolari, collaborazione, piano di rimedio.
- Strumenti: scanner automatici, strumenti di test manuali, strumenti di valutazione dei rischi. Nessus, OpenVAS, Qualys, Burp Suite e OWASP ZAP, Nmap

Assets in Energy

# Risorse nel settore energetico

Risorse: Generatori, Trasformatori, Sottostazioni, Linee di trasmissione
, Linee di distribuzione, Contatori, Sistemi di controllo

- Modbus
- DNP3 (Distributed Network Protocol 3)
- IEC 61850

Modbus: comunemente utilizzato per la comunicazione tra dispositivi di campo e sistemi di controllo

.

DNP3: prevalente nell'automazione dei servizi pubblici per i sistemi SCADA (Supervisory Control and Data Acquisition), in particolare nei sistemi di energia elettrica.

Questi protocolli facilitano:

- Scambio di dati
- Comandi di controllo
- Operazioni efficienti e affidabili all'interno delle infrastrutture energetiche.


# Modbus

Scopo: Modbus è un protocollo di comunicazione seriale comunemente utilizzato nelle applicazioni di automazione industriale, compreso il settore energetico. Facilita la comunicazione tra vari dispositivi elettronici quali controllori logici programmabili (PLC), sensori e contatori.

Funzionalità: Modbus utilizza un'architettura client-server in cui un dispositivo master (client) comunica con più dispositivi slave (server) tramite una connessione seriale. Supporta diversi tipi di dati e funzioni per la lettura e la scrittura di dati da/verso i registri all'interno dei dispositivi.

Applicazioni: nel settore energetico, Modbus è spesso utilizzato per il monitoraggio e il controllo delle risorse energetiche distribuite, come inverter solari, turbine eoliche e sistemi di accumulo di energia. Consente lo scambio di dati in tempo reale tra questi dispositivi e i sistemi di controllo di supervisione, permettendo agli operatori di monitorare le prestazioni e regolare le impostazioni secondo necessità.


# DNP3 (Distributed Network Protocol 3)

Scopo: DNP3 è un protocollo di comunicazione robusto e affidabile progettato specificamente per l'uso nei sistemi SCADA, in particolare nel settore dell'energia elettrica. Fornisce una comunicazione sicura ed efficiente tra i centri di controllo e i dispositivi remoti sul campo.

Funzionalità: DNP3 supporta vari tipi di dati e funzioni quali sincronizzazione temporale, segnalazione di eventi e autenticazione, rendendolo adatto per applicazioni infrastrutturali critiche. Funziona su vari mezzi di comunicazione, tra cui reti seriali (RS-232/485) e TCP/IP.

Applicazioni: nel settore energetico, DNP3 è ampiamente utilizzato per il monitoraggio e il controllo dei sistemi di generazione, trasmissione e distribuzione dell'energia elettrica. Consente alle utility di raccogliere dati in tempo reale da sottostazioni, contatori e altri dispositivi sul campo, consentendo un funzionamento efficiente della rete, il rilevamento dei guasti e la risposta.


# Negazione del servizio (DoS) Vulnerabilità

- CVE-2023-5462: Critico DoS vulnerabilità in XINJE XD5E-30R-E che causa il rifiuto del servizio.
- CVE-2023-5460: DoS dovuto a un overflow del buffer basato su heap in Delta Electronics WPLSoft.
- CVE-2023-1285: Condizione di condizione in Mitsubishi Electric India GC-ENET-COM che porta a DoS.
- CVE-2023-1150: Consumo incontrollato di risorse nella serie WAGO 750-3x/-8x.
- CVE-2022-37301: Denial of service dovuto a underflow di interi in SolaX Pocket WiFi.


# Vulnerabilità di overflow del buffer

- CVE-2023-5460: Basato su heap buffer basato su heap in Delta Electronics WPLSoft.
- CVE-2023-5462: Buffer overflow in Modbus Tools Modbus Poll.
- CVE-2022-4857: Overflow del buffer in Modbus Tools Modbus Poll.
- CVE-2022-4856: Overflow del buffer in Modbus Tools Modbus Slave.
- CVE-2021-39921: Overflow del buffer nel dissector Modbus di Wireshark.


# Vulnerabilità di bypass dell'autenticazione

- CVE-2022-45789: Bypass dell'autenticazione bypass in EcoStruxure Control Expert.
- CVE-2022-37300: Meccanismo di recupero password debole in vari prodotti.
- CVE-2021-22779: Bypass dell'autenticazione bypass in EcoStruxure Control Expert.
- CVE-2021-22772: Bypass dell'autenticazione in Easergy T200.
- CVE-2020-7523: Bypass dell'autenticazione in Schneider Electric Modbus Serial Driver.

Information Exposure

# Vulnerabilità relative all'esposizione delle informazioni

- CVE-2023-5461: Trasmissione in chiaro di informazioni sensibili in Delta Electronics WPLSoft.
- CVE-2022-30938: Corruzione della memoria che espone informazioni sensibili nel modulo Ethernet EN100.
- CVE-2022-30937: Corruzione della memoria che espone informazioni sensibili nel modulo Ethernet EN100.
- CVE-2021-22786: Esposizione di informazioni sensibili nella CPU Modicon M340 CPU.
- CVE-2019-7225: Credenziali non documentate che espone che espongono informazioni in ABB HMI.


# Codice Injection e vulnerabilità nella gestione dei privilegi

- CVE-2019-6549: Recupero delle credenziali in chiaro tramite FTP nel gateway Modbus PR100088.
- CVE-2019-6547: Accesso in lettura e scrittura ai valori Modbus senza autenticazione nel gateway Modbus PR100088.
- CVE-2019-6545: Recupero delle password tramite HTTP GET richiesta nel
  Gateway Modbus PR100088.
- CVE-2019-6543: FTP richiesta che causa un in PR100088 gateway Modbus.
- CVE-2020-7523: Escalation dei privilegi nel driver seriale Modbus
  Driver seriale Schneider Electric.


# Denial-of-Service in SIMATIC e SIPLUS

- CVE-2023-38380: interessa i prodotti SIMATIC e SIPLUS, causando un problema di Denial of Service dovuto a un rilascio di memoria errato nell'implementazione del server web.
- CVE-2022-43768: un'altra vulnerabilità di tipo denial-of-service nell'implementazione del server web dei prodotti SIMATIC e SIPLUS.
- CVE-2022-43767: vulnerabilità di tipo denial-of-service che interessa il server web dei prodotti SIMATIC e SIPLUS.
- CVE-2022-43716: influisce sulla funzionalità del server web nei prodotti SIMATIC e SIPLUS , che potrebbe causare una situazione di denial-of-service.
- CVE-2022-30938: interessa i moduli Ethernet EN100, causando il danneggiamento della memoria durante l'analisi dei pacchetti HTTP e provocando il crash delle applicazioni.

SCADA and IED

# Bypass dell'autenticazione nei dispositivi SCADA e IED

- CVE-2021-22772: i dispositivi della serie Easergy T200 consentono operazioni non autorizzate quando l'autenticazione viene bypassata. Ciò rappresenta un rischio significativo per la sicurezza, in quanto potrebbe consentire agli aggressori di ottenere il controllo non autorizzato su funzioni critiche.
- CVE-2020-6996: Le librerie Triangle MicroWorks DNP3 Outstation consentono agli aggressori di sfruttare un overflow del buffer basato su stack, che può potenzialmente portare ad un accesso non autorizzato ai sistemi interessati.
- CVE-2020-10613: Triangle MicroWorks SCADA Data Gateway consente agli aggressori remoti di divulgare informazioni sensibili a causa di una convalida impropria dei dati forniti dall'utente, compromettendo potenzialmente la riservatezza del sistema.
- CVE-2020-10611: STriangle MicroWorks SCADA Data Gateway consente agli aggressori remoti di eseguire codice arbitrario a causa di una convalida impropria dei dati forniti dall'utente, con il rischio di consentire l'accesso e il controllo non autorizzati al sistema.

# Grazie

Relatore: Stylianos Karagiannis (PDMFC, Portogallo) Si prega

di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com