KDFM eXplorer

DEVICE WEB ACCESS

Descrizione del processo Device Web Access DCA 4 consente a un utente con autorizzazioni adeguate di connettersi al server Web interno delle stampanti utilizzando la funzione denominata "Device Web Access", che presenta le seguenti specifiche tecniche e caratteristiche di sicurezza:

1. DCA4 riceve un comando di connessione Device Web Access da KDFM eXplorer Portal e verifica che la richiesta sia per una stampante gestita, quindi crea un tunneling SSH inverso.

2. Il Tunneling SSH inverso si basa sul protocollo SSH e viene creato dalla porta della stampante del servizio Web (tipicamente 80 o 443 o altro configurabile) a un server SSH remoto (porta 22 / SSH) raggiungibile tramite URL di dominio diversi appartenenti al dominio principale https://*.mpsmonitor.com.

3. Utilizzando il protocollo SSH, il sistema implementa un'autenticazione basata su chiave pubblica e crittografa le connessioni tra la stampante e gli endpoint del server SSH di KDFM eXplorer.

4. La connessione lato server viene creata come nuovo tunnel ad ogni richiesta di connessione, e terminata dopo ogni sessione, con una durata massima di 10 minuti. Le chiavi di sicurezza sono univoche per ogni installazione e ogni nuovo tunnel utilizza un ID sessione diverso per evitare il riutilizzo della sessione.

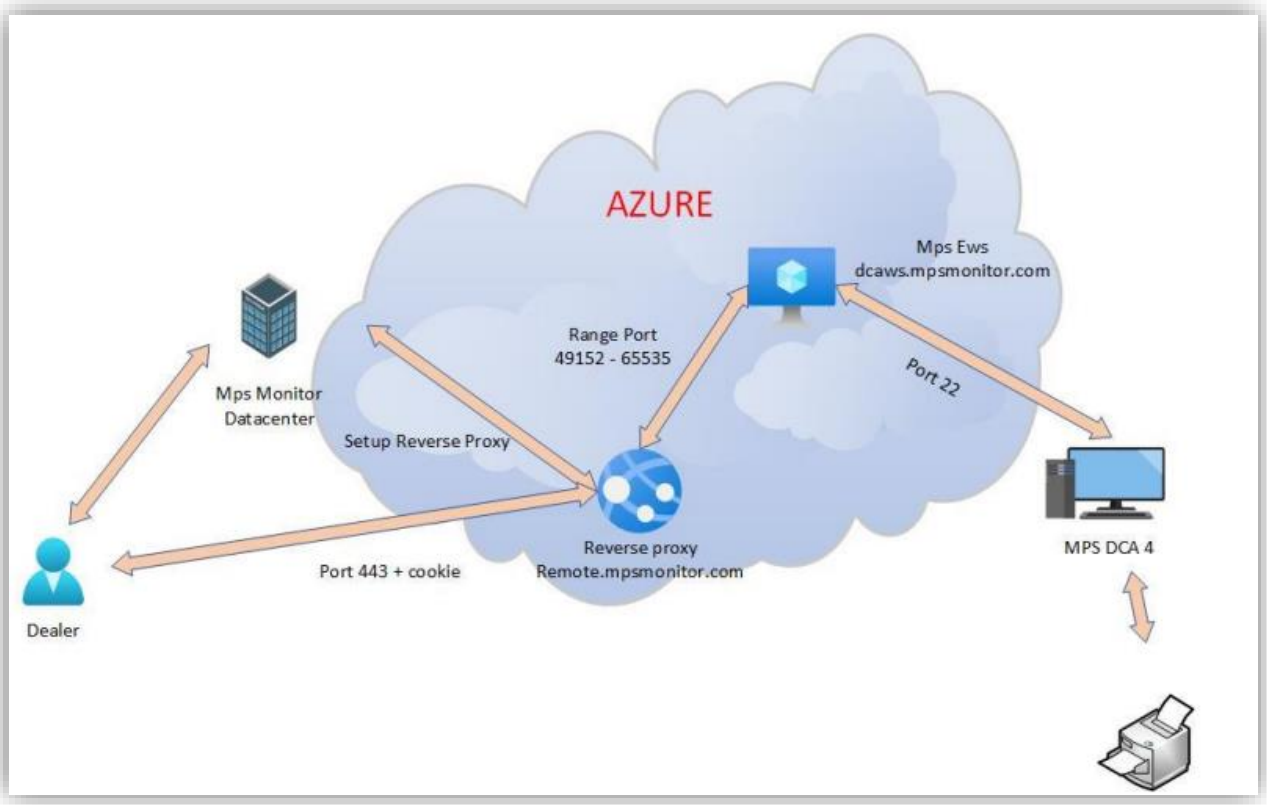
5. Viene implementata una complessa metodologia di autenticazione per garantire che tutte le parti coinvolte in ciascun tunnel SSH siano legittime e abbiano l'autorità per aprire e mantenere la connessione.

6. Prima dell'apertura del tunnel vengono effettuate alcune verifiche sul dispositivo per verificare che il dispositivo target corrisponda a quello su cui è stata richiesta la connessione. Se una di queste verifiche fallisce, il tunnel non è aperto.

7. La connessione Device Web Access è limitata solo a profili utente selezionati e può essere attivata solo da utenti con autenticazione avanzata al portale KDFM eXplorer (autenticazione a due fattori o Single Sign-On tramite Active Directory). Ciò impedisce l'utilizzo non autorizzato o dannoso della funzione di accesso Web al dispositivo in caso di furto delle credenziali.

8. Tutte le attività Web eseguite in Device Web Access vengono registrate sul server SSH. I clienti possono accedere ai log per verificare l'utilizzo di questa funzione da parte di altri utenti.

9. Device Web Access può essere disabilitato su ciascun cliente dall'utente nel portale KDFM eXplorer, o direttamente dall'interfaccia utente locale DCA 4, dal cliente stesso. Se la funzione è disabilitata nell'interfaccia utente DCA, non può essere riattivata dal Portale, garantendo così che ogni cliente abbia la possibilità di disabilitare questa funzione localmente dal sistema in cui è installato il DCA 4.



Descrizione del processo

PASSO 1
Il rivenditore connesso su kdfmportal.katun.com fa clic sulla stampante desiderata e richiede il DWA a un determinato dispositivo.

PASSO 2
Il portale genera un “Session id” che verrà utilizzato tra i vari componenti per il riconoscimento
la connessione.

PASSO 3
Il portale invia un comando al DCA per aprire la connessione tramite i seguenti parametri:
• Indirizzo IP e indirizzo Mac della stampante
• La porta dell'interfaccia Web della stampante (80 o 443) della stampante che deve essere inoltrata
• L'ID sessione per la connessione
• I parametri SSH
• Altri dettagli della stampante come numero di serie, marca e modello

PASSO 4

Il DCA ha ricevuto il comando:

1. Verifica che i dati della stampante siano uguali ai dati nel database locale e verifica che ~~lo~~ siano davvero di una stampante.

2. Utilizza il comando ssh.exe di Windows e apre un tunnel SSH su dcaws.mpsmonitor.com in uscita sulla porta 22

3. Avvisa il portale che il tunnel è attivo

PASSO 5

Il portale si collega a remote.mpsmonitor.com utilizzando un cookie che contiene il Session Id in modo che il proxy inverso possa inoltrare le richieste alla porta corretta sul server SSH.

Ora l'utente può lavorare sulla stampante