

Oggetto: Certificazione di Sicurezza e Conformità Normativa del software MPS Monitor DCA 4.x

Con la presente attestiamo che il software MPS Monitor DCA 4, interamente prodotto dalla nostra società, non contiene Virus, Malware, o minacce di alcun genere alla sicurezza informatica dei Clienti che lo utilizzano, e che l'installazione del DCA 4 all'interno della rete del Cliente non comporta né aggiunge rischi significativi per la sicurezza della rete stessa.

Il software DCA 4 è stato sviluppato in conformità alle specifiche e linee guida internazionali [OWASP Top 10](#) e viene sottoposto a continui test e verifiche da parte di enti indipendenti che ne certificano la conformità a tali linee guida.

Il codice del software DCA 4, prima del rilascio di ciascuna versione, viene sotto posto a Code Review ed analisi statica da parte di società specializzate nella fornitura di servizi di sicurezza informatica, al fine di verificare che:

- il pacchetto di installazione contenga esclusivamente moduli software firmati digitalmente da MPS Monitor srl in modo da garantirne l'autenticità
- il software non contenga vulnerabilità note ad elevata criticità, e che le vulnerabilità eventualmente riscontrate in precedenza, siano state eliminate prima del rilascio di ciascuna nuova versione
- Il software non venga rilevato come malware da parte dei più diffusi prodotti antivirus presenti sul mercato.

Tutti i metodi di accesso, le interfacce API e gli endpoint web utilizzati per la comunicazione tra il software DCA 4 ed i sistemi MPS Monitor in cloud sono sottoposti a Penetration Test con frequenza regolare, generalmente ogni trimestre, al fine di verificarne la sicurezza e la conformità agli standard ed alle linee guida internazionali. Il processo di aggiornamento automatico del software DCA 4 viene sottoposto a Penetration Test specifico con cadenza annuale per verificare la sicurezza contro possibili attacchi nella catena di aggiornamento. La funzionalità Device Web Access, essendo particolarmente critica dal punto di vista della sicurezza, è soggetta a specifiche attività di Penetration Test e verifiche approfondite.

Le informazioni raccolte tramite il software vengono trattate all'interno di un Sistema di Gestione della Sicurezza delle Informazioni che è certificato conforme alla norma UNI CEI ISO/IEC 27001/2017; il certificato n. 50 100 13777 Rev. 003 è stato emesso da TÜV Italia srl in data 06/03/2020 ed è disponibile a questo indirizzo: <http://www.mpsmonitor.it/docs/iso-27001.pdf>

La MPS Monitor srl adotta politiche di sicurezza delle informazioni conformi allo standard [AICPA SOC 2](#), e si sottopone ad Audit annuale da parte della società [A-LIGN](#) per attestare la compliance ai Trust Services Criteria definiti (**Security, Availability, Confidentiality**). Il Report di Audit SOC 2 rilasciato da A-LIGN è disponibile per il download nel Portale MPS Monitor previa firma elettronica di apposito Non Disclosure Agreement (NDA).

La MPS Monitor srl adotta politiche aziendali aventi come obiettivo il pieno rispetto dei requisiti normativi in materia di privacy e sicurezza delle informazioni, ed effettua trattamenti di dati pienamente conformi con le disposizioni dettate dal **Regolamento 2016/679/UE del Parlamento europeo e del Consiglio (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione dei dati. Con particolare riferimento al GDPR, il software MPS Monitor è prodotto ed operato nel rispetto dei principi stabiliti dalla normativa europea e, in particolare, dei principi di “*data protection by default and by design*”, perseguendo la tutela dei dati personali fino dalla fase di progettazione.

DCA 4 è stato sviluppato per raccogliere ed elaborare i dati relativi ai dispositivi di stampa collegati alla rete del Cliente, e per consentire una connessione in tempo reale tra utenti e dispositivi, al fine di gestirli in modo corretto ed efficace. Le operazioni effettuate sono direttamente connesse a questa specifica finalità. In particolare, il software non raccoglie dati relativi al contenuto dei documenti stampati, né a persone fisiche o giuridiche i cui dati sono trattati attraverso tali dispositivi e/o documenti.

Specifiche tecniche e descrizione del processo di raccolta dati

Il modulo software DCA 4 ha le seguenti specifiche tecniche e caratteristiche di sicurezza:

1. È installato su un dispositivo hardware (PC, Server, MAC o Raspberry) che esegue un sistema operativo supportato (Windows, Linux, Mac OS o Linux per Raspberry). Il dispositivo deve essere connesso alla rete del Cliente e deve avere accesso a Internet (porta 443 / HTTPS).
2. Per scambiare dati e ricevere informazioni sulle attività da eseguire, il software utilizza le chiamate HTTP2 GRPC (di solito inviate una volta ogni 5 minuti) e la connessione MQTT a un server che può essere raggiunto attraverso diversi URL di dominio appartenenti al dominio radice https://*.mpsmonitor.com. La connessione MQTT utilizza come default MQTT su WSS (porta 443). Può essere configurato anche per funzionare come una connessione MQTT standard (porta 8883)
3. A intervalli configurati e in base alle informazioni messe a disposizione dal server, il DCA 4 esegue scansioni UDP delle sottoreti, degli indirizzi IP o dei nomi host in cui è possibile raggiungere le stampanti; gli orari e le sottoreti o gli indirizzi IP o i nomi host da scansionare sono definiti in una funzione di amministrazione speciale nelle pagine di configurazione del portale MPS Monitor.

4. DCA 4 identifica tutti i dispositivi di tipo stampante, omettendo completamente tutti gli altri dispositivi di rete di qualsiasi altra natura.
5. La raccolta dei dati viene eseguita utilizzando UDP (porta 161) e richiede generalmente pochi secondi o minuti, a seconda della complessità della rete e del numero di dispositivi.
6. Utilizzando UDP, il traffico è minimo e non ha alcun impatto evidente sulla rete e sui dispositivi.
7. I dati raccolti dalle stampanti sono archiviati localmente in un database. Le modifiche ai dati memorizzati localmente vengono inviate tramite HTTPS al server MPS Monitor. Sia i dati archiviati localmente che i dati inviati su Internet sono crittografati.

Descrizione del processo "Device Web Access"

DCA 4 consente all'utente con autorizzazioni adeguate di connettersi al Web Server interno delle stampanti utilizzando la funzione denominata "Device Web Access", che ha le seguenti specifiche tecniche e funzionalità di sicurezza:

1. DCA4 riceve un comando di connessione Device Web Access dal portale MPS Monitor e verifica che la richiesta sia relativa a una stampante gestita, quindi crea un tunneling SSH inverso.
2. Il tunneling SSH inverso si basa sul protocollo SSH ed è creato dalla porta della stampante del servizio Web (in genere 80 o 443, o altra porta disponibile) ad un server SSH remoto (porta 22 / SSH) che può essere raggiunto attraverso diversi URL di dominio appartenenti al dominio radice 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 MPS Monitor.
4. La connessione lato server viene creata come un nuovo tunnel ad ogni richiesta di connessione e termina dopo ogni sessione, con una durata massima di 10 minuti. Le chiavi di sicurezza sono uniche per ciascuna installazione del DCA 4, ed ogni nuovo tunnel utilizza un diverso ID di sessione per evitare il riutilizzo delle sessioni.
5. Viene applicata una complessa metodologia di autenticazione per garantire che tutte le parti coinvolte in ciascun tunnel SSH siano legittime e abbiano l'autorizzazione ad aprire e mantenere la connessione.
6. Prima dell'apertura del tunnel vengono effettuate numerose verifiche sui dati del dispositivo per verificare che il dispositivo di destinazione corrisponda a quello su cui è stata richiesta la connessione. Se una di queste verifiche fallisce, il tunnel non viene aperto.
7. La connessione Device Web Access è limitata solo ad alcuni profili utente autorizzati, e può essere attivata solo da utenti con autenticazione forte al portale MPS Monitor (autenticazione a due fattori o Single Sign-On tramite Active Directory). Ciò impedisce l'utilizzo non autorizzato o dannoso della funzione Device Web Access in caso di furto di credenziali.
8. Tutte le attività web svolte all'interno di Device Web Access sono loggate sul server SSH. I clienti possono accedere ai log per verificare l'utilizzo di questa funzione da parte di altri utenti.
9. L'accesso Web del dispositivo può essere disattivato su ciascun cliente dall'utente nel portale MPS Monitor o direttamente dall'interfaccia utente locale DCA 4 dal cliente stesso. Se la funzione è disattivata nell'interfaccia utente locale del DCA 4, 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.

Integrazione dei sistemi di Print Management

DCA 4 permette anche, se installato su una rete dove è presente un sistema di Print Management (come ad esempio PaperCut MF/NG o sistemi simili) di essere configurato per raccogliere ed elaborare dati relativi ai job di stampa ed agli utenti che stampano, con l'obiettivo di fornire funzionalità di Business Intelligence ed Analytics su tali dati.

Questo avviene tramite il seguente processo:

1. DCA 4 può essere configurato per accedere ad una cartella sulla rete del cliente dove il sistema di Print Management esporta file di testo / CSV contenenti i dati dei job di stampa
2. Quando questi file sono creati, DCA 4 li raccoglie e li invia al sistema MPS Monitor in cloud, per elaborarli
3. I dati presenti nei file elaborati sono aggiunti al Database principale di MPS Monitor e vengono resi disponibili agli utenti autorizzati nella sezione Analytics del sistema, per permettere la creazione di specifici report e dashboard di Business Intelligence
4. Se i file contengono dati relativi al contenuto dei documenti stampati (come nomi dei file oppure altre informazioni potenzialmente confidenziali) tali dati vengono eliminati prima di essere importati nel Database, per garantire che nessuna informazione personale o confidenziale è mantenuta all'interno del sistema MPS Monitor in conseguenza di questo processo.

Milano, 24 Marzo 2022

MPS Monitor srl
L' Amministratore Unico
Nicola De Blasi



MPS Monitor Srl

Sede Legale: Via Borromei 2 – 20123 Milano

Sede Operativa: Via Cipri, 1 - 25100 Brescia

PEC: mpsmonitor@legalmail.it - P.Iva / CF: 03122040987