QRM Security Statement

Informazioni sulla sicurezza del sistema QRM

Quality in Electronic Manufacturing
www.qem.it
QEM

Indice generale

1. Informazioni

1.1 Specificazioni

I diritti d'autore di questo manuale sono riservati. Nessuna parte di questo documento, può essere copiata o riprodotta in qualsiasi forma senza la preventiva autorizzazione scritta della QEM .

QEM non presenta assicurazioni o garanzie sui contenuti e specificatamente declina ogni responsabilità inerente alle garanzie di idoneità per qualsiasi scopo particolare. Le informazioni in questo documento sono soggette a modifica senza preavviso. QEM non si assume alcuna responsabilità per qualsiasi errore che può apparire in questo documento.

Marchi registrati :
- QEM® è un marchio registrato.

1.2 Validità

Il presente documento è valido integralmente salvo errori od omissioni.

1.2.1 Release

Release documento	Descrizione	Data
0	Nuovo documento.	17/02/2011

2. Avvertenze

Questo documento è diretto agli amministratori di rete professionisti. Le informazioni contenute nel presente documento sono di natura prettamente tecnica e particolareggiate. Grazie a queste informazioni, i professionisti IT hanno a disposizione, prima di installare il prodotto QNet SDK, un'immagine dettagliata relativamente alla sicurezza del software.

3. Funzionalità

Il prodotto QNet SDK, e più precisamente il programma QEM Resources Manager (QRM), permette ad un computer di condividere, attraverso la rete protetta gestita dal QEM Remote Control (QRC), alcune proprie risorse locali con altri computer con installato il medesimo software QNet SDK ed aventi precise credenziali di accesso.

Tutte le risorse condivise sono atte a permettere la comunicazione con i prodotti QEM delle famiglie QMove, MicroQMove e QMove+ sfruttando il protocollo di comunicazione BIN1.

4. La sicurezza

Il programma QRM, installato con il prodotto QNet SDK, è utilizzato per fornire un accesso sicuro ed immediato via Internet a chi deve controllare un apparato QEM per fornire assistenza remota ad uno sviluppatore o per operare aggiornamenti dei programmi applicativi oppure per operazioni di raccolta dati.

All'utente remoto non saranno permessi accessi ad alcun'altra risorsa del PC con cui ha instaurato la connessione.

È evidente che una funzionalità di tale portata seppur limitata, nella potenziale carenza di sicurezza di Internet, deve essere protetta in diversi modi contro eventuali attacchi e per questo ogni connessione stabilita viene cifrata.

5. Funzionamento di una connessione

La rete QNet è composta dai seguenti componenti:

- Nodes: nodi della rete (istanze del programma QRM. Una per ogni PC fisico o macchina virtuale).
- Resources, risorse del nodo (risorse dichiarate localmente in un nodo che potranno essere pubbliche o private).
- Gestore dei nodi (programma QRC in esecuzione su servers QEM e gestore della rete QNet).
- Client: utilizzatore del nodo (programma o tool che si connette al nodo per accedere alle risorse locali/remote).
- Signature Keys: chiavi di firma (sono chiavi che permettono di accedere alla propria sottorete nel sistema QNet).

Ogni nodo (istanza QRM) può dichiarare un numero illimitato di risorse locali che andranno ad identificare una connessione fisica con un prodotto QMove collegato a tale sistema (tramite connessione seriale RS-232/422 o indirizzo IP). Le risorse potranno essere di tipo privato o pubblico. Le risorse private potranno essere utilizzate solamente dai client del nodo locale. Le risorse pubbliche, una volta che il QRM attiva la connessione con la rete QNet, saranno visibili ed utilizzabili da tutti i componenti della rete appartenenti alla stessa sotto-rete e quindi in possesso delle stesse signature keys.

Lo scopo della QNet è quello di poter instaurare una connessione peer-to-peer tra due PC (nodi) affinché le risorse dichiarate localmente di uno siano accessibili all'altro.
Quando il client del nodo A decide di voler utilizzare una risorsa del nodo B chiede al gestore dei nodi (QRC) di instaurare la connessione. Il QRC crea quindi una VPN tra il nodo A ed il nodo B. A questo il gestore dei nodi ha finito il proprio compito e non è più partecipe ai dati transitanti.

Tutti i nodi della rete (istanze QRM) sono collegati allo stesso gestore (server QRC) ma non visibili tra loro a meno che non condividano una o più signature key. Le signature key sono particolari file crittografati creati dal personale QEM che devono essere installati nel proprio nodo e che permettono quindi di creare la propria sottorete. Ogni nodo può avere più di una signature key e quindi appartenere a differenti sottoreti. Le signature key hanno poi alcuni flag di configurazione che permettono ad un nodo di appartenere ad una sottorete, e quindi vederne le risorse remote, ma di non condividere le proprie risorse con la stessa.

Come descritto più avanti nel paragrafo "Crittografia e autenticazione", nemmeno noi, in qualità di operatori dei server di instradamento, possiamo leggere il traffico di dati crittografati, inoltre il traffico dati tra due peer non passa dai nostri server ma è diretta tra le due controparti.

5.1 Porte di comunicazione

Il QRM per lavorare utilizza una serie di porte TCP/IP ed UDP locali e remote. Vediamo ora l'elenco e modalità di utilizzo:

localhost:3000	listening del server TCP/IP presente nel QRM su cui è basata la comunicazione client <-> QRM. Questa porta è indispensabile per il corretto funzionamento del QRM sia in modalità locale che remota.
qrc.q-move.eu:8000	il QRM crea una connessione TCP/IP in uscita verso l'indirizzo qrc.q-move.eu:8000 dove il QRC implementa il TCP/IP server di gestione dei nodi della rete. Questo accesso è necessario perché il QRM possa accedere ai nodi remoti.
qrc.q-move.eu:8001	il QRM crea una connessione UDP in uscita verso l'indirizzo qrc.q-move.eu:8001 dove il QRC implementa un server UDP di mediazione dei peers necessaria ad instaurare la connessione VPN.
any:any	il QRM crea una connessione UDP ogni volta che deve attivare una VPN con una risorsa di un nodo remoto. La porta UDP utilizzata è random in quanto viene chiesto al sistema operativo di fornire la prima disponibile. Per prima cosa il QRM inizia la fase di richiesta connessione conversando con il mediatore in qrc.q-move.eu:8001, poi quando entrambi i peer si sono manifestati la stessa porta instaura la VPN con il peer dell'altro nodo.
qrc.q-move.eu:5010	il QRC implementa un server FTP che permette al QRM di avviare una procedura automatica di aggiornamento del software.

Riassumendo il QRM ha al suo interno un server TCP/IP in ascolto della porta locale 3000 ed utilizzato per comunicare con i programmi client. Tale server e porta DEVE ed E' utilizzata solamente localmente e quindi non deve essere resa pubblica all'esterno del PC ove il QRM viene eseguito.

Il QRM si connette al QRC tramite un TCP/IP client (in uscita) all'indirizzo qrc.q-move.eu:8000. Questa connessione serve a trasmettere ciclicamente informazioni sulle risorse al QRC che poi le distribuirà ai vari nodi della sottorete di appartenenza. Nessuna informazione che non sia attinente alle risorse pubbliche viene inviata in questa fase.

Il QRM utilizza una porta UDP random in uscita, prima all'indirizzo qrc.q-move.eu:8001 (mediazione) e poi all'indirizzo del peer per la creazione della VPN utilizzata per l'interscambio dati tra i due peer.

Il QRM si connette al QRC tramite un TCP/IP client (in uscita) all'indirizzo qrc.q-move.eu:5010 (ove risiede un server ftp) per le operazioni di auto aggiornamento del software stesso.

Tutte le connessioni verso la rete internet vengono instaurate in uscita. Nessuna porta deve essere abilitata in ingresso.

5.2 Crittografia e autenticazione

Il QRM implementa vari livelli di crittografia dei pacchetti inviati al QRC e ai nodi (peer della VPN) in condivisione di risorse. La crittografia è basata sullo scambio di chiave pubblica/privata e può essere considerata completamente sicura secondo gli standard attuali. Poiché la chiave privata non lascia mai il computer client, questa procedura assicura che i computer interconnessi, inclusi i servers di instradamento di QEM, non possano decifrare il flusso di dati.

6. Sicurezza dell'applicazione

6.1 Nessuna modalità nascosta

Non esiste alcuna modalità che consenta al QRM di funzionare come processo di background nascosto. Sebbene nell'installazione del QWorkbench, o di QNet SDK, venga visualizzata l'opzione “Start Qem Resources Manager service” in realtà il QRM non è basato su servizi NT ma è un normale programma eseguibile, mentre con questa dicitura si intende richiedere all'utente la conferma alle operazioni di auto-esecuzione del QRM ad ogni avvio del sistema operativo.

Una volta avviato, il QRM, è sempre visibile come icona nell'area di notifica delle applicazioni: ciò significa che il QRM è deliberatamente non idoneo al monitoraggio nascosto di computer o di dipendenti.

Quando il QRM viene avviato assume lo stato di inattivo (Offline) per ciò che riguarda la connessione alla rete QNet. Ciò significa che dev'essere espressamente l'utente a porlo in stato Online con la rete QNet. L'utente può mettere in connessione il QRM alla rete QNet tramite il bottone di connessione sul pannello grafico o tramite il menu ' Connect Node to QNet '.

Nessun client al QRM della Qem (QView, QPaint) mette in connessione il QRM alla QNet in modo autonomo.