Exploitability	L'attacco, sia esso condotto sul piano dell'interruzione fisica della connessione o sul piano dell'interruzione logica del flusso dei dati, è complesso.	1
Affected Users	100% (la piattaforma è resa indisponibile).	3
Discoverability	L'attaccante dovrà impegnare parecchie risorse per organizzare l'attacco.	1

DREAD Score: 8/15 (MEDIO)

7.2.8 Elevazione di privilegi attraverso l'esecuzione remota di codice da parte del 'Web Server'

Categoria: Elevation Of Privilege

Descrizione: 'Client Browser' potrebbe essere in grado di eseguire codice in remoto sul sistema ' Web Server'.

Contromisure:

- Il processo non deve contenere percorsi che mandano in esecuzione dati presi dal flusso di input (es. il nome di un eseguibile).
- Se un processo manda in esecuzione dati presi dal flusso di input, questi devono essere convalidati in modo da escludere che venga eseguito codice arbitrario.

Valutazione della priorità della minaccia (Ranking)

DREAD	Descrizione	Score
Damage Potential	L'attaccante potrebbe prendere il controllo dell'intero sistema, attraverso tecniche di "lateral moving" (il "lateral moving" di solito comporta attività legate alla ricognizione <<information gathering>>, furto di credenziali e spostamenti su altri computer).	3
Reproducibility	L'attacco può essere condotto in qualunque momento.	3
Exploitability	Per la natura del servizio, l'attacco richiede un'utenza autenticata. Si richiedono anche skill elevati.	1
Affected Users	100% (se l'esito finale fosse effettivamente il controllo del sistema).	3
Discoverability	L'attaccante dovrà impegnare parecchie risorse per scoprire la vulnerabilità sfruttabile (l'attacco di norma sfrutta una catena di debolezze).	1

DREAD Score: 11/15 (MEDIO)

7.2.9 Elevazione dei privilegi attraverso il cambiamento del flusso di esecuzione nel codice del 'Web Server'

Categoria: Elevation Of Privilege

Descrizione: Un attaccante può passare dati al 'Web Server' in modo da cambiare a suo vantaggio il flusso di esecuzione del programma all'interno del 'Web Server' stesso.

Contromisure:

- Convalidare in modo appropriato gli input e gestire le eccezioni per evitare percorsi di esecuzione imprevisti.
- Impiegare meccanismi di protezione contro il buffer overflow e altri problemi di gestione della memoria.
- Applicare principio del minimo privilegio.