

BOLLETTINO DI SICUREZZA XEROX XRX06-006

Aggiornamento cumulativo che risolve varie vulnerabilità delle funzioni di sicurezza.

Le versioni del software di sistema 12.060.17.000, 14.060.17.000 o 13.060.17.000, a seconda che il prodotto sia un WorkCentre[®] o un WorkCentre[®] Pro, sono un aggiornamento alle versioni del software di sistema 12.050.03.000, 14.050.03.000 e 13.050.03.000, rispettivamente, e comprendono correzioni al software di sistema. Vedere l'Appendice A per ottenere il software di sistema *.060.17.000 ¹.

Si consiglia vivamente di aggiornare il software di sistema caricato sul dispositivo alla versione 12.060.17.000, 14.060.17.000 o 13.060.17.000, rispettivamente. Per ottenere il software di sistema aggiornato, attenersi alla procedura descritta nell'Appendice A. Per aggiornare il dispositivo, seguire le istruzioni di installazione per il cliente fornite con il software di sistema. La tabella che segue indica la versione corrispondente del controller di rete per ciascuna delle tre versioni del software di sistema.

Prodotti	Versione SW di sistema	Versione controller di rete
WorkCentre 232/238/245/255/265/275	12.060.17.000.	040.022.00115
WorkCentre Pro 232/238/245/255/265/275	13.060.17.000.	040.022.50115
WorkCentre 232/238/245/255/265/275 con opzione PostScript	14.060.17.000.	040.022.10115

Rischio

Le versioni 12.060.17.000, 14.060.17.000 e 13.060.17.000 del software di sistema sono release di mantenimento che comprendono soluzioni a problemi di sicurezza delle versioni 1 del software di sistema 12.050.03.000, 14.050.03.000 e 13.050.03.000, rispettivamente. L'aggiornamento comprende soluzioni alle seguenti vulnerabilità delle funzioni di sicurezza presenti nel codice del controller di rete/ESS e del server Web MicroServer:

- Nome host TCP/IP nell'interfaccia utente web vulnerabile ad attacchi di tipo "command injection".
- Campo nome della cartella di scansione su mailbox nell'interfaccia utente web vulnerabile ad attacchi di tipo "command injection".
- Parametri di configurazione dei Servizi di rete Microsoft nell'interfaccia utente web vulnerabili ad attacchi di tipo "command injection".
- Le autorizzazioni del browser potrebbero consentire accessi non autorizzati.
- L'opzione di configurazione automatica TFTP/BOOTP potrebbe consentire la configurazione non autorizzata delle impostazioni.
- Le richieste di servizi web possono essere eseguite utilizzando HTTP invece di HTTPS.
- La firma dei messaggi e-mail può essere contraffatta per visualizzare elementi errati.
- La funzione di scansione su mailbox potrebbe consentire lo scaricamento anonimo non autenticato di file protetti.
- Il dispositivo non mantiene l'ora con precisione, di conseguenza la data e l'ora dei registri di controllo sono errate.

Se sfruttate, queste vulnerabilità impedirebbero un corretto funzionamento delle funzioni di protezione e un utente non autorizzato riuscirebbe ad accedere al sistema e a cambiarne la configurazione. Le password del cliente e dell'utente non sono esposte a questo rischio.

Oltre alle correzioni riportate sopra, è stata migliorata la sicurezza dei file di aggiornamento DLM mediante l'integrazione di firme digitali.

¹* corrisponde a 12, 13 o 14, a seconda che il prodotto sia un WorkCentre[®] o un WorkCentre[®] Pro

Prodotti a rischio:

WorkCentre[®]	WorkCentre[®] Pro
232	232
238	238
245	245
255	255
265	265
275	275

Appendice A**Come ottenere l'ultima versione del software di sistema**

Per ottenere la versione generica più recente:

- a) Mediante un browser accedere al sito www.xerox.com.
- b) Selezionare il collegamento "Supporto e Driver".
- c) Selezionare "Multifunzione".
- d) Selezionare "WorkCentre" o "WorkCentre Pro", a seconda del modello utilizzato.
- e) Individuare il collegamento corrispondente al proprio modello di WorkCentre.
- f) Selezionare "Driver e Download".
- g) Selezionare il collegamento "Aggiornamenti per prodotti".
- h) Selezionare il collegamento "System software version xx.xx.xx.xxx install instructions" e stampare o salvare queste istruzioni.
- i) Selezionare il collegamento "System Software Upgrade Version xx.xx.xx.xxx" e salvare il file sul computer.
- j) Dopo aver scaricato il file, estrarne il contenuto sul desktop.
- k) Consultare il file delle istruzioni per l'installazione del software di sistema salvato ("System Software Install Instructions"), che contiene importanti informazioni sull'aggiornamento del dispositivo.
- l) Aggiornare il dispositivo.
- m) Tornare alla sezione relativa all'installazione della patch del documento citato sopra.

Dichiarazione di non responsabilità

Le informazioni contenute in questo documento Xerox sono fornite "così come sono" senza alcuna garanzia. Xerox Corporation non riconosce alcuna garanzia, espressa o implicita, comprese le garanzie di commerciabilità e idoneità a uno scopo specifico. In nessun caso Xerox Corporation sarà responsabile di danni di qualsiasi tipo risultanti dall'uso dell'utente o dal mancato rispetto delle informazioni fornite in questo documento Xerox, inclusi danni speciali, diretti, indiretti, incidentali, conseguenti o perdita di profitti aziendali, anche nel caso in cui Xerox Corporation sia stata informata della possibilità di tali danni. Alcuni paesi non consentono l'esclusione o la limitazione della responsabilità per i danni conseguenti, di conseguenza le limitazioni di cui sopra potrebbero non essere applicabili.