

BOLLETTINO DI SICUREZZA XEROX XRX07-002

Il controller di rete/ESS e il server Web MicroServer sono vulnerabili agli attacchi di tipo "command injection". Se scoperta e sfruttata, questa vulnerabilità permette l'esecuzione in remoto di software arbitrario.

In passato, questo problema è stato risolto con il Bollettino di sicurezza XRX06-005. La soluzione offerta nel bollettino, che ha comportato il rilascio di una patch (P29) e di software per il dispositivo in grado di risolvere il problema di sicurezza, è comunque troppo restrittiva per quanto riguarda il limite massimo di caratteri utilizzati per le impostazioni di rete dei dispositivi. Ciò ha causato problemi con alcuni clienti o nell'ambito di particolari applicazioni che utilizzano caratteri speciali, ad esempio il carattere di sottolineatura, nei nomi degli host di rete.

Il dispositivo potrebbe essere già protetto. Se il proprio sistema soddisfa già i requisiti minimi di sicurezza (oppure contiene già la patch P29 rilasciata con il bollettino XRX06-005) e funziona correttamente (e non si utilizzano caratteri speciali come il carattere di sottolineatura nei nomi degli host di rete) non occorrerà installare questa patch.

P31 è classificata come patch **importante**.

La soluzione software è disponibile come file ZIP di 1.1 MB dal collegamento:

http://www.xerox.com/downloads/usa/en/c/cert_P31v14_ESS_Network_Controller_CP_Patch.zip

La patch può essere installata direttamente dal cliente. Per installare la patch e proteggere i dati riservati da possibili attacchi attraverso la rete, seguire le istruzioni a pagina 2.

Rischio

Nell'ambito dei controlli costanti esercitati da Xerox per proteggere i clienti da potenziali attacchi, è stata scoperta la seguente vulnerabilità:

- Nome host TCP/IP nell'interfaccia utente Web vulnerabile ad attacchi di tipo "command injection"

Questa vulnerabilità del codice del controller di rete/ESS e del server Web potrebbe consentire a un utente non autorizzato di aggirare la procedura di autenticazione e di eseguire software arbitrario in remoto.

Di conseguenza, un pirata informatico potrebbe apportare modifiche non autorizzate alla configurazione del sistema. Le password del cliente e degli utenti non sono tuttavia a rischio.

Questa patch si applica solo ai modelli connessi in rete¹ dei seguenti prodotti:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	

¹Se il prodotto non è collegato alla rete, non è vulnerabile agli attacchi, pertanto non è richiesta alcuna azione preventiva.

Soluzione

Installazione della patch WebUI Ultima modifica: 02 ottobre 2007

La patch può essere installata sul sistema seguendo le istruzioni riportate di seguito.

Riepilogo delle versioni e delle procedure:

- Stabilire la versione iniziale del software di sistema o la versione del controller ESS
- Stabilire quali sono gli aggiornamenti necessari
- Eseguire l'aggiornamento dei dispositivi in base alle esigenze
- Applicare la patch, se necessario

Istruzioni per WorkCentre®/WorkCentre Pro® 232/238/245/255/265/275

Utilizzare la patch WCP275_WC7665_P31v14.dlm nel file cert_P31v14_ESS_Network_Controller_CP_Patch.zip

	Se la versione del software è SW sistema o Controller ESS		Installare la patch?	Passaggio successivo:	Quindi:	Nuovo numero del controller di rete/ESS:
1	Da *.27.24.000 a *.27.24.020	Da 040.010.#0930 a 040.010.#1160	No	Eseguire l'aggiornamento a *.60.22.000 o versione successiva. Vedere l'Appendice A per informazioni su come ottenere questa versione	Vedere la NOTA 1 di seguito	Se la patch non viene applicata 040.022.#1031 Se la patch viene applicata, 040.022.#1031.BIOSxx.xx.P31v14
2	Da *.50.03.000 a *.50.03.009	Da 040.010.#1172 a 040.010.#2250	No	Eseguire l'aggiornamento a *.60.22.000 o versione successiva. Vedere l'Appendice A per informazioni su come ottenere questa versione	Vedere la NOTA 1 di seguito	Se la patch non viene applicata, 040.022.#1031. Se la patch viene applicata, 040.022.#1031.BIOSxx.xx.P31v14.
3	*.50.03.011	040.010.#2280	No	Rivolgersi all'assistenza per eseguire l'aggiornamento a *.60.22.000 o versione successiva	Vedere la NOTA 1 di seguito	Se la patch non viene applicata, 040.022.#1031. Se la patch viene applicata, 040.022.#1031.BIOSxx.xx.P31v14
4	*.27.24.015 (con certificazione Common Criteria)	040.010.#1121	No	Eseguire l'aggiornamento a *.60.17.000	Vedere la NOTA 1 e la NOTA 2 di seguito	040.022.#0115
5	*.39.24.001 Certificazione Common Criteria	040.010.#1123	No	Eseguire l'aggiornamento a *.60.17.000	Vedere la NOTA 1 e la NOTA 2 di seguito	040.022.#0115
6	*.60.15.000	040.022.#0112	No	Eseguire l'aggiornamento a *.60.22.000 o versione successiva Vedere l'Appendice A	Vedere la NOTA 1 di seguito	Se la patch non viene applicata, 040.022.#1031. Se la patch viene applicata, 040.022.#1031.BIOSxx.xx.P31v14.
7	*.60.17.000 (con certificazione Common Criteria)	040.022.#0115	Sì	Vedere la NOTA 1 e la NOTA 2 di seguito	N/A	Se la patch viene applicata, 040.022.#0115.P31v14
8	Da *.60.17.000 a *.60.22.005	Da 040.022.#0115 a 040.022.#1090	Sì	Vedere la NOTA 1 di seguito	N/A	Se la patch non viene applicata, da 040.022.#1031 a 040.022.#1090. Se la patch viene applicata, da 040.022.#1031.BIOSxx.xx.P31v14 a 040.022.#1090.BIOSxx.xx.P31v14.
9	*.60.22.006 e versione superiore	040.022.#1100 o versione superiore	N/A	Fatto	N/A	N/A

Istruzioni per WorkCentre® 7655/7665

Utilizzare la patch WCP275_WC7665_P31v14.dlm nel file cert_P31v14_ESS_Network_Controller_CP_Patch.zip

	Se la versione del software è SW sistema o Controller di rete		Installare la patch?	Passaggio successivo:	Quindi:	Nuovo numero del controller di rete/ESS:
1	Da 040.032.50855 a 040.032.51040	Da 040.032.50855 a 040.032.51030	No	Rivolgersi all'assistenza tecnica per eseguire l'aggiornamento o alla versione 040.032.53080	Vedere la NOTA 1 di seguito	Se la patch viene applicata, 040.032.53080.BIOSxx.xx.P31v14
2	040.032.53080 con certificazione Common Criteria	040.032.53080	Sì	Vedere la NOTA 1 e la NOTA 2 di seguito	N/A	Se la patch viene applicata, 040.032.53080.BIOSxx.xx.P31v14
3	Da 040.032.55030 a 040.032.55061	Da 040.032.55030 a 040.032.55060	Sì	Vedere la NOTA 1 di seguito	N/A	Se la patch viene applicata, da 040.032.55030.BIOSxx.xx.P31v14 a 040.032.55060.BIOSxx.xx.P31v14
4	040.032.55070 e versione superiore	040.032.55070	N/A	Fatto	N/A	N/A

NOTA 1: il dispositivo sarà ora protetto contro il rischio di violazione di sicurezza descritto in questo bollettino. Tuttavia, se si riscontra che le limitazioni per i caratteri sono troppo restrittive per il proprio ambiente e si desidera implementare un set di caratteri più ampio (garantendo simultaneamente una protezione contro questo tipo di violazione di sicurezza), caricare la patch P31(WCP275_WC7665_P31v14.dlm) sul dispositivo.

NOTA 2: il dispositivo ha ottenuto la certificazione Common Criteria. Se si carica la patch P31(WCP275_WC7665_P31v14.dlm) sul dispositivo per implementare un set di caratteri più ampio (vedere a proposito la Nota 1), il dispositivo perderà la certificazione Common Criteria.

Installazione della patch

È necessario scaricare la patch. La patch è compressa in formato ZIP. Scaricare il file ZIP dall'URL indicato ed estrarre tutto il contenuto sul desktop.

Metodi di installazione della patch

La patch di aggiornamento (come la maggior parte del software) può (e deve) essere installata dal cliente. È possibile eseguire l'installazione seguendo vari metodi.

- Metodo Software macchina (Aggiornamento): inviare un file di aggiornamento/patch al dispositivo utilizzando la pagina Web del dispositivo
- Comando LPR: applicare l'aggiornamento/patch a un singolo dispositivo utilizzando un comando LPR.
- Batch di comandi LPR: applicare l'aggiornamento/patch a vari dispositivi utilizzando un batch di comandi LPR.
- XDM e CenterWare Web: inviare i file di aggiornamento/patch a vari dispositivi tramite XDM e CenterWare Web.

Per ulteriori informazioni sui metodi riportati sopra, vedere il suggerimento "How to Upgrade, Patch or Clone Xerox Multifunction Devices" (Come eseguire l'aggiornamento, l'invio di patch o la clonazione per i dispositivi multifunzione Xerox)(<http://www.office.xerox.com/support/dctips/dc06cc0410.pdf>)

Metodo Software macchina (Aggiornamento)

- 1) Aprire un browser Web e connettersi al dispositivo multifunzione immettendo l'indirizzo IP del dispositivo.
- 2) Selezionare l'icona "Indice" in alto al centro sullo schermo.
- 3) Selezionare "Software macchina (Aggiornamenti)".
- 4) Inserire il nome utente e la password del dispositivo.
- 5) In "Aggiornamento manuale", selezionare il pulsante Sfoglia per individuare e poi selezionare il file **WCP275_WC7665_P31v14.dlm**.
- 6) Fare clic sul pulsante "Installa software".
- 7) A questo punto, tutti i sistemi WCP stamperanno un foglio di installazione della patch e poi si riavvieranno automaticamente per installare la patch. Quando **.P31vxx** viene aggiunto al numero di versione del controller di rete (ESS), significa che la patch è installata.

Appendice A - Come ottenere la versione *.60.22.000 (o successiva) del software di sistema

Per ottenere le versioni *.60.22.000 (o successive) del software di sistema:

- a) Aprire un browser Web per accedere al sito www.xerox.com.
- b) Selezionare il collegamento "Supporto e Driver".
- c) Selezionare "Multifunzione".
- d) In base al modello che si possiede, selezionare "WorkCentre" o "WorkCentre Pro".
- e) Individuare il collegamento che corrisponde al proprio modello di WorkCentre.
- f) Selezionare "Driver e Download".
- g) Selezionare il collegamento "Aggiornamenti per i prodotti".
- h) Selezionare il collegamento "System software set *.60.22.000 Install Instructions" e stampare il documento (oppure salvarlo).
- i) Selezionare il collegamento per "System Software set *.60.22.000" 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 ("System Software Install Instructions") salvato prima.
- l) Eseguire l'aggiornamento del dispositivo.

Declinazione di 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 per danni di qualsiasi tipo risultanti dall'utenza o dal mancato rispetto delle informazioni fornite in questo documento Xerox, inclusi danni speciali, diretti, indiretti, incidentali, conseguenti o perdita di profitti aziendali, anche qualora 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, pertanto le limitazioni di cui sopra potrebbero non essere applicabili.