

BOLLETTINO DI SICUREZZA XEROX XRX06-005

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

Di seguito, sono riportate una soluzione software (patch P29) e le istruzioni per installarla sui prodotti indicati. La patch può essere installata direttamente dal cliente. Attenersi alle istruzioni per installarla e proteggere i propri dati riservati da possibili attacchi attraverso la rete.

La soluzione software è compressa in un file ZIP di 59 KB e può essere scaricata mediante il seguente collegamento nella pagina del sito Xerox relativa alla sicurezza (Xerox.com/Security):

http://www.xerox.com/downloads/usa/en/c/cert_P29_WC2xx-Only_HTTP.zip

I clienti che desiderano eliminare questa vulnerabilità del sistema sui prodotti elencati di seguito devono, innanzi tutto, attenersi alle istruzioni seguenti per verificare se dispongono di SMP1 (software di sistema versione 12.50.03.000, 13.50.03.000 o 14.50.03.000, a seconda che il prodotto sia un WorkCentre® o un WorkCentre® Pro) o versione successiva. Se la versione del software di sistema non è *.50.03.000¹ o successiva, scaricare il software dalla sezione Driver e Download del sito www.xerox.com. Consultare l'Appendice A delle istruzioni per l'installazione della patch per informazioni su come ottenere il software di sistema *.50.03.000.

Nota: questa patch di sicurezza è contrassegnata dal codice **P29**. Dopo l'installazione della patch, il controller di rete riporterà la versione del BIOS del dispositivo e **.P29** (Ad es. 40.010.#1172.BIOS07.07.P29²)

Contesto

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

- Attacco di tipo "command injection" tramite l'interfaccia Web sul nome host TCP/IP

Questa vulnerabilità, rilevata nel codice del controller di rete/ESS e del server web, potrebbe consentire a un pirata informatico di aggirare la procedura di autenticazione e di eseguire in remoto del software arbitrario.

Un pirata informatico potrebbe apportare modifiche non autorizzate alla configurazione del sistema. Le password del cliente e dell'utente non sono a rischio.

Riconoscimenti:

Xerox desidera ringraziare:

- Steve Puls, Rajat Mandal e Mike Webb che hanno sviluppato e testato questa patch.
- Brendan O'Connor per aver portato a nostra conoscenza l'esistenza di vulnerabilità.

Prodotti su cui si può utilizzare questa patch:

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

Nota: questa vulnerabilità non si presenta sui WorkCentre® 7655 / 7665.

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

² # corrisponde a 0, 1 o 5 a seconda che il prodotto sia un WorkCentre® o un WorkCentre® Pro

Soluzione**Istruzioni di installazione**Nome file della patch: **P29_WC2xx-Only_HTTP.dlm**

Questa patch può essere installata facilmente nel giro di qualche minuto seguendo le istruzioni riportate di seguito.

Riepilogo delle versioni e delle procedure:

	Se la versione del software è SW sistema o Controller di rete		Installo la patch?	Passaggio seguente:	Quindi:	Dicitura del controller di rete/ESS:
1	Da *.27.24.000 a *.27.24.014	Da 040.010.#0930 a 040.010.#1110	NO	Eseguire l'aggiornamento a *.50.03.000 Vedere Nota 2 di seguito	Applicare la patch P29	Eseguire l'aggiornamento, quindi leggere la riga 3 di seguito
2	Da *.27.24.016 a *.27.24.020	Da 040.010.#1120 a 040.010.#1160	Si	Installare la patch P29	Fatto	Da 040.010.#1120.BIOS07.07.P29 a 040.010.#1160.BIOS07.07.P29
3	Da *.50.03.000 a *.50.03.009	Da 040.010.#1172 a 040.010.#2250	Si	Installare la patch P29	Fatto	Da 040.010.#1172.BIOS07.07.P29 a 040.010.#2250.BIOS07.07.P29
4	*.50.03.011 o versione successiva	040.010.#2280 o versione successiva	Soluzione al problema incorporata	Fatto	-	040.010.#2280 o versione successiva
5	*.27.24.015 (con certificazione Common Criteria)	040.010.#1121	Si	Vedere la NOTA 1 di seguito	Fatto	040.010.#1120.BIOS07.07.P29
6	*.39.24.001 Certificazione Common Criteria	040.010.#1123	Si	Vedere la NOTA 1 di seguito	Fatto	040.010.#1123.BIOS07.07.P29

NOTA 1: se il software di sistema caricato sul proprio dispositivo è *.27.24.015 o *.39.24.001³, significa che il dispositivo ha ottenuto la certificazione Common Criteria. Il dispositivo è pronto per accettare la patch P29. Se lo si desidera, si può caricare la patch P29, anche se questa installazione invalida la certificazione Common Criteria.

³ Versione 040.010.*1121 o 040.010.*1123 del controller di rete
701P45975

Verifica della versione del software di sistema

Per determinare la versione del software di sistema, è possibile stampare un rapporto di configurazione oppure visualizzare la versione sull'interfaccia del client Web.

Per stampare un rapporto di configurazione dall'interfaccia utente locale della macchina:

- 1) Premere il pulsante Condizione macchina.
- 2) Selezionare "Stampa rapporto configurazione adesso".
- 3) Selezionare "Stampa rapporto configurazione sistema".
- 4) Cercare il numero della versione del software di sistema.

Per visualizzare la versione sull'interfaccia del client Web:

- 1) Aprire un browser Web e collegarsi al dispositivo multifunzione immettendo l'indirizzo IP del dispositivo.
- 2) Selezionare l'icona "Indice" che si trova nella parte centrale dello schermo, in alto.
- 3) Selezionare "Configurazione".
- 4) Scorrere fino a "Impostazione" per visualizzare la versione del software di sistema.

NOTA 2: se il software di sistema installato non rientra tra le versioni indicate, seguire le istruzioni riportate nell'Appendice A per scaricare e aggiornare il software di sistema PRIMA di installare la patch.

Installazione della patch

- 1) Aprire un browser web e connettersi al dispositivo multifunzione immettendo l'indirizzo IP del dispositivo.
- 2) Selezionare l'icona "Indice" che si trova nella parte destra dello schermo, in alto.
- 3) Selezionare l'aggiornamento manuale.
- 4) Selezionare il file Sfoglia per individuare e selezionare il file **P29_WC2xx-Only_HTTP.dlm (accertarsi che il file non sia zippato (P29_WC2xx-Only_HTTP.ZIP.))**
- 5) Premere il pulsante per installare il software.
- 6) Inserire il nome utente (Admin) e la password dell'amministratore per il dispositivo.
- 7) WorkCentre si riavvia automaticamente per installare la patch.
- 8) La patch è installata quando **.BIOSxx.yy.P29 (xx.yy è la versione del BIOS sul dispositivo)** viene aggiunto al numero della versione del controller di rete.
Il modello di WorkCentre riporta la versione solo nella pagina web di configurazione e solo se la versione del software di sistema è *.50.03.000 o superiore.

La patch è stata installata correttamente su questo sistema.

Appendice A

Come ottenere il software di sistema *.50.03.000

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 che si possiede.
- e) Individuare il collegamento corrispondente al proprio modello di WorkCentre.
- f) Selezionare "Driver e Download".
- g) Selezionare il collegamento "Aggiornamenti per i prodotti".
- h) Selezionare il collegamento "System software version *.50.03.000 install instructions" e stampare il documento (oppure salvarlo).
- i) Selezionare il collegamento "System Software Upgrade Version *.50.03.000" e salvare il file sul computer.
- j) Dopo aver scaricato il file, estrarne il contenuto sul desktop.
- k) Consultare il documento dc06cc0406.pdf incluso nel pacchetto scaricato per informazioni sull'aggiornamento del dispositivo.
- l) Consultare il file delle istruzioni per l'installazione del software di sistema ("System Software Install Instructions") salvato.
- m) Aggiornare il dispositivo.
- n) Ritornare alla sezione "Installazione della patch".

<Fine delle istruzioni>

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 potrà essere ritenuta 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, consequenziali 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 consequenziali, di conseguenza le limitazioni di cui sopra potrebbero non essere applicabili.