

XEROX-SICHERHEITSMERKBLATT XRX08-001

Der ESS/Netzwerkcontroller weist Sicherheitslücken auf, die von Angreifern zur Ausführung von beliebigem Code mit Hilfe präparierter RPC-Anfragen (Remoteprozeduraufruf) missbraucht werden könnten.

Patch P32 wird als Softwarelösung mit Installationsanweisungen für die unten genannten Produkte bereitgestellt. Dieses Korrekturprogramm ist vom Benutzer zu installieren. Die Softwarelösung ist in einer ZIP-Datei mit 8,3 MB komprimiert und kann über diesen Link heruntergeladen werden:

http://www.xerox.com/downloads/usa/en/c/cert_P32v2_WCP275_WC7665_Patch.zip

Patch P32 wurde als **wesentliche** Softwarekorrektur eingestuft.

Die beigefügten Anweisungen enthalten Angaben zu den Versionen, für welche die Korrektursoftware erforderlich ist, sowie zum Vorgehen bei der Patchinstallation.

- Bei Geräten der Serie WorkCentre®/WorkCentre® Pro 2xx enthält die Systemsoftwareversion *.60.22.007 oder höher (ESS Controller-Version 040.022.x1110 oder höher) bereits die Fehlerkorrektur und der Patch muss nicht installiert werden.
- Bei Geräten der Serie WorkCentre® 7655/7665 enthält die Systemsoftwareversion 040.032.55080 oder höher (ESS Controller-Version 040.032.55080 oder höher) bereits die Fehlerkorrektur und der Patch muss nicht installiert werden. Beim WorkCentre® 7655/7665 mit einer Systemsoftware, die nicht mindestens Version 040.032.53080 (Netzwerkcontrollerversion 040.022.*1031) entspricht, ist die Aktualisierung auf Version 040.032.53080 durch einen Wartungstechniker erforderlich, bevor der Patch installiert werden kann.

Hinweis: Dieser Sicherheitspatch trägt die Bezeichnung **P32**. Nach der Patchinstallation enthält die Versionsangabe für den Netzwerkcontroller den Zusatz **.P32** (z. B. 040.022.x0115.P32).

Hintergrund

Im Rahmen der ständigen Bemühungen zum Schutz seiner Kunden hat Xerox folgende Sicherheitslücken aufgedeckt:

- CVE-2007-2446: potenzieller Heap-Überlauf, der die Remoteausführung von beliebigem Schadcode ermöglicht
- CVE-2007-2447: Möglichkeit zur Remote Command Injection

Diese Schwachstellen im ESS/Netzwerkcontroller, welcher die Datei- und Druckerfreigabedienste für SMB- bzw. CIFS-Clients (dazu gehören Xerox-MFGs) steuert, könnten von Angreifern zur Ausführung von beliebigem Schadcode mit Hilfe präparierter RPC-Anfragen (Remoteprozeduraufruf) missbraucht werden.. Ein Risiko besteht dabei nur für die Druckerfreigabedienste. Angreifern kann es u. U. gelingen, unerlaubte Änderungen an der Systemkonfiguration vorzunehmen. Kunden- und Benutzerkennwörter sind jedoch nicht gefährdet.

Dieses Korrekturprogramm gilt für vernetzte Versionen¹ der folgenden Produkte:

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

¹Wenn das Gerät nicht ans Netzwerk angeschlossen ist, besteht keine Gefahr und es müssen keine Maßnahmen getroffen werden.

Lösung

Installationsanweisungen

Name der Patch-Datei: **WCP275_WC7665_P32v2.dlm**

Dieses Korrekturprogramm kann wie nachfolgend beschrieben auf dem System installiert werden.

Versionen und erforderliche Handlungen:

- Aktuelle Systemsoftwareversion oder ESS Controller-Version feststellen
- Feststellen, welche Aktualisierungen erforderlich sind
- Geräte nach Bedarf aktualisieren
- Falls erforderlich, Patch installieren

Für WC/WCP 232/238/245/255/265/275

	Softwareversion entspricht Systemsoftware oder ESS-Controller		Patch-installation erforderlich ?	Nächster Schritt:	Dann:	Versionsangabe für Netzwerkcontroller/ESS jetzt wie folgt:
1	*.27.24.000 bis *.27.24.020	040.010.#0930 bis 040.010.#1160	Nein	Auf Version *.60.22.000 oder höher aktualisieren. Siehe Anhang A	Patch P32 laden	040.022.#1031.BIOSxx.xx.P32v2
2	*.50.03.000 bis *.50.03.009	040.010.#1172 bis 040.010.#2250	Nein	Auf Version *.60.22.000 oder höher aktualisieren. Siehe Anhang A	Patch P32 laden	Nach Patchinstallation: 040.022.#1031.BIOSxx.xx.P32v2
3	*.50.03.011	040.010.#2280	Nein	Kundendienst zum Aktualisieren auf *.60.22.000 oder höher anfordern	Patch P32 laden	Nach Patchinstallation: 040.022.#1031.BIOSxx.xx.P32v2
4	*.27.24.015 nach Common Criteria zertifiziert	040.010.#1121	Nein	Siehe HINWEIS 1 unten	-	-
5	*.39.24.001 Nach Common Criteria zertifiziert	040.010.#1123	Nein	Siehe HINWEIS 1 unten	-	-
6	*.60.15.000	040.022.#0112	Nein	Auf Version *.60.22.000 oder höher aktualisieren Siehe Anhang A	Patch P32 laden	040.022.#1031.BIOSxx.xx.P32v2
7	*.60.17.000 nach Common Criteria zertifiziert	040.022.#0115	Ja	Siehe HINWEIS 1 unten	-	Nach Patchinstallation: 040.022.#0115.P32v2
8	*.60.17.000 bis *.60.22.006	040.022.#0115 bis 040.022.#1100	Ja	Patch P32 laden	-	040.022.#0115.BIOSxx.xx.P32v2 bis 040.022.#1100.BIOSxx.xx.P32v2
9	*.60.22.007 und höher	040.022.#1110 oder höher	N/V	Fertig	-	-

HINWEIS 1: Für die Systemsoftwareversionen *.27.24.015, *.39.24.001 und *.60.17.000 entspricht die Konfiguration der Zertifizierung nach den Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie). Auf Wunsch kann auf *.60.17.000 aktualisiert und dann Patch P32 geladen werden, die Zertifizierung des Geräts nach den Common Criteria geht damit jedoch verloren.

Für WC 7655/7665

	Softwareversion entspricht Systemsoftware oder Netzwerkcontroller		Patch-installation möglich?	Nächster Schritt:	Dann:	Versionsangabe für Netzwerkcontroller/ESS jetzt wie folgt:
1	040.032.50855 bis 040.032.51040	040.032.50855 bis 040.032.51030	Nein	Kundendienst zum Aktualisieren auf 040.032.53080 anfordern	Patch P32 laden	040.032.53080.BIOSxx.xx.P32v2
2	040.032.53080	040.032.53080	Ja	Patch P32 laden	-	040.032.53080.BIOSxx.xx.P32v2
3	040.032.53080 nach Common Criteria zertifiziert	040.032.53080	Ja	Siehe HINWEIS 1 unten	-	Nach Patchinstallation: 040.032.53080.BIOSxx.xx.P32v2
4	040.032.55030 bis 040.032.55070	040.032.55030 bis 040.032.55070	Ja	Siehe HINWEIS 1 unten	-	Nach Patchinstallation: 040.032.55030.BIOSxx.xx.P32v2 bis 040.032.55070.BIOSxx.xx.P32v2
5	040.032.55080 und höher	040.032.55080	N/V	Fertig	-	-

HINWEIS 1: Für Systemsoftwareversion 040.032.53080 entspricht die Konfiguration der Zertifizierung nach den Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie). Es kann Patch P29 geladen werden, die Zertifizierung des Geräts nach den Common Criteria geht damit jedoch verloren.

Patchinstallation

Der Patch muss heruntergeladen werden. Der Patch ist im ZIP-Format komprimiert. Die ZIP-Datei über den angegebenen URL herunterladen und den Inhalt auf den Desktop extrahieren. Nicht versuchen, die Datei mit der Erweiterung .DLM zu öffnen. Diese Datei ist der Patch, der im unveränderten Zustand auf das Multifunktionsgerät geladen werden muss.

Vorgehensweisen für die Patchinstallation

Dieser Patch und die Aktualisierungssoftware können und sollten (wie Software i. A.) nach Möglichkeit vom Benutzer installiert werden. Für die Installation existieren verschiedene Verfahren.

- Senden einer Aktualisierungs-/Patchdatei an das Gerät mit Hilfe der Geräte-Webseite für die Gerätesoftware-Aktualisierung
- Aktualisieren/Patchen eines einzelnen Geräts mit Hilfe eines LPR-Befehls
- Aktualisieren/Patchen mehrerer Geräte mit Hilfe eines LPR-Befehlsstapels
- Verwendung von XDM und CenterWare Web zum Senden von Aktualisierungs-/Patch-Dateien an mehrere Geräte

Weitere Informationen zu den oben genannten Methoden befinden sich im Kundentipp „How to Upgrade, Patch or Clone Xerox Multifunction Devices“ (Aktualisieren, Nachbessern und Klonen von Xerox-Multifunktionsgeräten) unter <http://www.office.xerox.com/support/dctips/dc06cc0410.pdf>.

Geräte-Software-Methode (Aktualisierung)

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen.
- 2) Das Indexsymbol im oberen mittleren Fensterbereich auswählen.
- 3) „Geräte-Software (Aktualisierungen)“ auswählen.
- 4) Benutzernamen und Kennwort des Geräts eingeben.
- 5) Unter „Manuelle Aktualisierung“, die Schaltfläche „Durchsuchen“ und anschließend die Datei **WCP275_WC7665_P32v2.dlm** auswählen.
- 6) „Software installieren“ auswählen.
- 7) Auf dem WCP wird ein Patch-Installationsblatt ausgegeben und automatisch ein Neustart durchgeführt, um den Patch zu installieren. Bei erfolgreicher Patchinstallation wird die Versionsnummer des Netzwerkcontrollers (ESS) durch die Angabe **.P32v2** erweitert.

Anhang A – Beschaffung der Systemsoftwareversion

Zum Beschaffen der Systemsoftwareversionen *.60.22.000 oder höher wie folgt vorgehen:

- a) In die Adresszeile des Internetbrowsers www.xerox.com eingeben.
- b) Auf den Link „Support und Treiber“ klicken.
- c) „Multifunktion“ auswählen.
- d) Je nach Modell „WorkCentre“ bzw. „WorkCentre Pro“ auswählen.
- e) Den Link für das betreffende WorkCentre-Modell suchen.
- f) „Treiber & Downloads“ auswählen.
- g) Den Link für „Geräteaufrüstungen und –aktualisierungen“ auswählen.
- h) Den Link mit Installationsanweisungen für Systemsoftwaresatz *.60.22.000 anklicken und die Anleitung ausdrucken bzw. speichern.
- i) Den Link für den Systemsoftwaresatz *.60.22.000 anklicken und die Datei auf dem Computer speichern.
- j) Nach dem Herunterladen die Dateien in ein Verzeichnis auf dem Rechner extrahieren.
- k) Die gespeicherten Anweisungen zur Systemsoftwareinstallation durchsehen.
- l) Das Gerät aufrüsten.

Anhang B – Aktivierung von LPD, Drucken über Anschluss 515

Für die Patchübertragung mit der LPR-Methode muss das Multifunktionsgerät LPD (Line Printer Daemon) über Anschluss 515 unterstützen. Bei den meisten Multifunktionsgeräten ist diese Option standardmäßig aktiviert. Ggf. LPD-Druck zur Verwendung der LPR-Methode aktivieren.

Zur Aktivierung von LPD die folgenden Schritte ausführen:

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen.
- 2) Das Index- oder Geräteindexsymbol im oberen Bereich der Anzeige auswählen.
- 3) „LPR/LPD“ bzw. „Line Printer Daemon“ auswählen.
- 4) Das Feld „Aktiviert“ muss markiert sein.
- 5) „Anwenden“ auswählen.
- 6) Benutzernamen Admin und Admin-Kennwort eingeben und „OK“ auswählen.
- 7) Multifunktionsgerät entweder von der Webseite „Status“ oder durch Drücken des Netzschalters am Multifunktionsgerät neu starten.

Haftungsausschluss

Die Informationen in diesem Dokument werden im „Ist-Zustand“ ohne Gewähr zur Verfügung gestellt. Die Xerox Corporation übernimmt keinerlei Gewährleistungen, weder explizit noch implizit, einschließlich Gewährleistungen der allgemeinen Gebrauchstauglichkeit und Eignung für einen bestimmten Zweck. In keinem Fall haftet die Xerox Corporation für Schäden jeglicher Art, die durch Nutzung des Benutzers oder Nichtbeachtung der in diesem Dokument enthaltenen Informationen entstanden sind, einschließlich direkter, indirekter, beiläufig entstandener oder Folgeschäden, Gewinnausfällen sowie konkreter Schäden, selbst wenn die Xerox Corporation auf die Möglichkeit derartiger Schäden hingewiesen wurde. Die Gesetzgebung mancher Länder verbietet den Haftungsausschluss bzw. die Haftungsbeschränkung bei Folgeschäden, so dass die vorgenannten Beschränkungen ggf. nicht zutreffend sind.