

## XEROX SICHERHEITSBULLETIN XRX07-001

Der ESS/Netzwerkcontroller weist Sicherheitslücken auf, die zur Remoteausführung beliebiger Software, zur Fälschung von digitalen Zertifikaten oder zur Auslösung von Denial of Service-Angriffen missbraucht werden könnten.

Die folgende Softwarelösung (Patch P30) mit Installationsanweisungen wird für die nachfolgend genannten Produkte bereitgestellt. Dieses Korrekturprogramm ist vom Benutzer zu installieren. Bei der Patch-Installation zum Schutz Ihres Gerätes vor möglichen Angriffen über das Netzwerk wie nachfolgend beschrieben vorgehen.

Die Softwarelösung ist in einer ZIP-Datei mit 990 KB komprimiert und kann über diesen Link heruntergeladen werden:

[http://www.xerox.com/downloads/usa/en/c/cert\\_P30\\_ESS\\_Network\\_Controller\\_Patch.zip](http://www.xerox.com/downloads/usa/en/c/cert_P30_ESS_Network_Controller_Patch.zip)

Um die Sicherheitslücke für die u. g. Produkte zu schließen, sollte zunächst anhand der beigefügten Installationsanweisungen geprüft werden, dass die korrekte Version zur Installation des Patches vorliegt. Bei Geräten der Serie WC/WCP 2xx enthält die Systemsoftwareversion \*.60.22.000 oder höher (ESS Controller-Version 040.022.\*1031 oder höher) bereits die Fehlerkorrektur und die Installation des Patches ist nicht erforderlich.

Die Installationsanweisungen für die erforderlichen Schritte aufmerksam lesen, welche durchgeführt werden müssen, falls die betreffende Version niedriger als die oben angegebenen ist. Außerdem muss beim WorkCentre® 7655/7665 mit Systemsoftware unter Version 040.032.53080 (Net-Controller-Version 040.022.\*1031 oder höher) ein Wartungstechniker angefordert werden, um das Gerät auf die Systemsoftware-/Net-Controller-Version 040.032.53080 zu aktualisieren, bevor der Patch installiert werden kann.

Hinweis: Dieser Sicherheitspatch trägt die Bezeichnung **P30**. Nach der Patch-Installation enthält die Versionsangabe für den Netzwerkcontroller den Zusatz **.P30** (z. B. 40.010.#1172.P30). Wie bereits erwähnt, enthält bei Geräten der Serie WC/WCP 2xx die Systemsoftwareversion \*.60.22.000 oder höher (ESS Controller-Version 040.022.\*1031 oder höher) bereits die Fehlerkorrektur und die Installation des Patches ist nicht erforderlich.

### Hintergrund

Im Rahmen der ständigen Bemühungen zum Schutz von Kunden hat Xerox folgende, in Red Hat Security Advisory RHSA-2006:0695-12 dokumentierte Sicherheitslücken bei OpenSSL aufgedeckt:

- Missbräuchlicher Bounds Check (Feldgrenzenüberprüfung) von Benutzereingaben
- Missbräuchlicher Umgang mit Fehlerbedingungen
- Unangemessene Verarbeitung von digitalen Signaturen
- Unsachgemäße Validierung der Länge von öffentlichen Schlüsseln
- Unsicherer Umgang mit Peer-to-Peer-Protokollen

Diese Sicherheitslücken im ESS/Netzwerkcontroller erlauben Angreifern u. U. die Umgehung der Authentifizierung und die Remoteausführung beliebiger Software, die Fälschung von Zertifikaten oder das Auslösen von Denial of Service-Angriffen gegen das Gerät.

Angreifer sind dann theoretisch in der Lage, unerlaubte Änderungen an der Systemkonfiguration vorzunehmen. Kunden- und Benutzerkennwörter sind jedoch nicht gefährdet.

**Geräte, auf die der Patch anwendbar ist:**

**WorkCentre® WorkCentre® Pro**

232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	

Lösung

**Installationsanweisungen**

Name der Patch-Datei: **P30.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 möglich?	Nächster Schritt:	Dann:	Versionsangabe für Netzwerkcontroller/ESS jetzt wie folgt:
<b>1</b>	*.27.24.000 bis *.27.24.020	040.010.#0930 bis 040.010.#1160	Nein	Auf Version *.60.17.000 aktualisieren Siehe Anhang A	Siehe Reihe 8	-
<b>2</b>	*.50.03.000 bis *.50.03.009	040.010.#1172 bis 040.010.#2250	Nein	Auf Version *.60.17.000 aktualisieren Siehe Anhang A	Siehe Reihe 8	-
<b>3</b>	*.50.03.011	040.010.#2280	Nein	Kundendienst zum Aktualisieren auf *.60.22.000 oder höher anfordern	-	040.022.#1031
<b>4</b>	*.27.24.015 nach Common Criteria zertifiziert	040.010.#1121	Nein	S. HINWEIS 1 unten	-	-
<b>5</b>	*.39.24.001 Nach Common Criteria zertifiziert	040.010.#1123	Nein	S. HINWEIS 1 unten	-	Nach Patch- Installation: 040.022.#0115.P3 0

6	*.60.15.000	040.022.#0112	Nein	Auf Version *.60.22.000 oder höher aktualisieren Siehe Anhang A	-	040.022.#1031
7	*.60.17.000 nach Common Criteria zertifiziert	040.022.#0115	Ja	S. Hinweis 2 unten	-	Nach Patch-Installation: 040.022.#0115.P30
8	*.60.17.000 bis *.60.17.006	040.022.#0115 bis 040.022.#1022	N/V	Patch P30 laden Oder Auf Version *.60.22.000 oder höher aktualisieren . Siehe Anhang A	-	040.022.#1031
9	*.60.17.008	040.022.#1031	N/V	Fertig	-	-
10	*.60.22.000 und höher	040.022.#1031	N/V	Fertig	-	-

**HINWEIS 1:** Für Systemsoftwareversion \*.27.24.015 oder \*.39.24.001 entspricht die Konfiguration der Zertifizierung nach den Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie). Auf Wunsch kann auf x.60.17.000 aktualisiert und dann Patch P30 geladen werden (Reihe 7 oben), die Zertifizierung des Geräts nach den Common Criteria geht damit jedoch verloren.

**HINWEIS 2:** Für Systemsoftwareversion \*.60.17.000 entspricht die Konfiguration einer **baldigen** Zertifizierung nach den Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie). Auf Wunsch kann PatchP30 geladen werden, **die** Zertifizierung des Geräts nach den Common Criteria geht jedoch verloren, **sobald die Zertifizierung abgeschlossen wurde.**

### 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 P30 laden	040.032.53080.P30
2	040.032.53080	040.032.53080	Ja	Patch P30 laden	-	040.032.53080.P30
3	040.032.53080 nach Common Criteria zertifiziert	040.032.53080	Ja	S. HINWEIS 1 unten	-	Nach Patch-Installation: 040.032.53080.P30
4	040.032.55030 und höher	040.032.55030 und höher	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). Auf Wunsch kann Patch P30 geladen werden (siehe Reihe 2 oben), die Zertifizierung des Geräts nach den Common Criteria geht damit jedoch verloren.

## Installation des Patches

Der Patch muss heruntergeladen werden. Der Patch ist im ZIP-Format komprimiert. Die ZIP-Datei vom angegebenen URL herunterladen und den gesamten 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 Patch-Installation

Dieser Patch und die Aktualisierung (wie die meisten Softwareprogramme) kann und sollte vom Kunden installiert werden. Hierzu gibt es verschiedene Vorgehensweisen.

- Senden einer Aktualisierungs-/Patch-Datei an das Gerät anhand der Geräte-Webseite für die Gerätesoftware-Aktualisierung
- Aktualisieren/Patchen eines einzelnen Geräts mithilfe eines LPR-Befehls
- Aktualisieren/Patchen mehrerer Geräte mithilfe 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 oder 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 Bereich des Bildschirms in der Mitte auswählen.
- 3) "Geräte-Software (Aktualisierungen)" auswählen.
- 4) Benutzername und Kennwort des Geräts eingeben.
- 5) Unter "Manuelle Aktualisierung" die Schaltfläche "Durchsuchen" und anschließend die Datei P30.dlm auswählen.
- 6) "Software installieren" auswählen.
- 7) Auf allen WCPs wird ein Patch-Installationsblatt ausgedruckt und automatisch ein Neustart durchgeführt, um den Patch zu installieren. Bei erfolgreicher Patch-Installation wird die Versionsnummer des Netzwerkcontrollers (ESS) durch die Angabe **.P30** erweitert.

## Anhang A

### Beschaffung der Systemsoftwareversion \*.50.03.000

Zum Beschaffen der Systemsoftwareversionen \*.60.17.000, \*.60.22.000 oder höher wie folgt vorgehen:

- a) In die Adresszeile des Internetbrowsers [www.xerox.com](http://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 Systemsoftwareversion XXX anklicken (wobei XXX für die zutreffende Systemsoftwareversion wie in den obigen Installationsanweisungen angegeben steht) und die Anleitung ausdrucken bzw. speichern.
- i) Den Link für "Systemsoftware-Aktualisierungsversion XXX" anklicken (wobei XXX für die zutreffende Systemsoftwareversion wie in den obigen Installationsanweisungen angegeben steht) und die Datei auf dem Rechner 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.

### Haftungsausschluss

Die in dieser Xerox Produktantwort enthaltenen Informationen werden im "Istzustand" ohne Gewährleistungen jeglicher Art zur Verfügung gestellt. Die Xerox Corporation übernimmt keinerlei Gewährleistungen, weder explizit noch implizit, einschließlich Gewährleistungen der Markttauglichkeit 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 dieser Xerox Produktantwort enthaltenen Informationen entstanden sind, einschließlich direkter, indirekter, zufälliger, Folge-, Verlust von Geschäftsgewinnen oder speziellen Schäden, selbst wenn die Xerox Corporation auf die Möglichkeit derartiger Schäden hingewiesen wurde. Einige Staaten/Länder verbieten den Ausschluss oder die Beschränkung der Haftung für Folgeschäden, so dass diese Beschränkungen u. U. nicht auf Sie zutreffen.