

30.11.2006

XEROX-SICHERHEITSMERKBLATT XRX06-006

Kumulatives Update zur Schließung mehrerer Sicherheitslücken

Bei den Versionen 12.060.17.000, 14.060.17.000 und 13.060.17.000 der Systemsoftware für das WorkCentre® bzw. das WorkCentre® Pro handelt es sich um kumulative Updates für die Systemsoftwareversionen 12.050.03.000, 14.050.03.000 und 13.050.03.000 mit Sicherheitskorrekturen. Siehe Anhang A zur Beschaffung der *.060.17.000-Systemsoftware¹.

Die Aktualisierung auf Systemsoftwareversion 12.060.17.000, 14.060.17.000 bzw. 13.060.17.000 wird dringend empfohlen. Zur Beschaffung der aktualisierten Systemsoftware die Vorgehensweisen in Anhang A befolgen. Die Geräteaktualisierung mithilfe der Kundeninstallationsanweisungen durchführen, die mit der Software bereitgestellt werden. In der folgenden Tabelle ist die Version des Netzwerkcontrollers für die jeweilige Systemsoftwareversion angegeben.

Produkte	Systemsoftwareversion	Netzwerkcontrollerversion
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 mit PostScript-Option	14.060.17.000.	040.022.10115

Hintergrund

Versionen 12.060.17.000, 14.060.17.000 und 13.060.17.000 der Systemsoftware stellen Wartungsversionen mit Sicherheitskorrekturen für die Systemsoftwareversionen 12.050.03.000, 14.050.03.000 bzw. 13.050.03.000 dar. Die Aktualisierung enthält Patches für folgende Sicherheitslücken im ESS/Netzwerkcontroller und MicroServer-Webservercode:

- Der TCP/IP-Hostname in der Webbenutzeroberfläche ist anfällig für Command-Injection-Angriffe.
- Das Namensfeld des Zielordners für die Funktion "Scan-to-Mailbox" in der Webbenutzeroberfläche ist anfällig für Command-Injection-Angriffe.
- Parameter der Microsoft-Netzwerkconfiguration in der Webbenutzeroberfläche sind anfällig für Command-Injection-Angriffe.
- Durch Browserberechtigungen können unbefugte Zugriffe ermöglicht werden.
- Über die Option zur automatischen Konfiguration von TFTP/BOOTP können möglicherweise Konfigurationseinstellungen unbefugt geändert werden.
- Webserviceanforderungen können über HTTP anstelle von HTTPS übermittelt werden.
- Signaturen von E-Mailnachrichten können zur Anzeige missbräuchlicher Objekte zweckentfremdet werden.
- Über die Funktion "Scan-to-Mailbox" wird eventuell der anonyme, nicht authentifizierte Download geschützter Dateien ermöglicht.
- Aufgrund ungenauer Zeitaufzeichnung des Geräts enthalten Prüfprotokolle falsche Zeitstempel.

Durch Ausnutzung dieser Sicherheitslücken werden Sicherheitsfunktionen u. U. beeinträchtigt. Angreifer könnten dann Zugriff auf das System erlangen und unerlaubte Änderungen an der Systemkonfiguration vornehmen. Kennwörter von Kunden und Benutzern sind nicht gefährdet.

Zusätzlich zur Beseitigung der oben erwähnten Schwachstellen wurde die Sicherheit der DLM-Upgrade Dateien durch die Einbindung digitaler Signaturen optimiert.

¹ * 12, 13 oder 14, je nachdem, ob es sich bei dem Gerät um ein WorkCentre® oder ein WorkCentre® Pro handelt

30.11.2006

30.11.2006

Betroffene Produkte:

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

Anhang A

Beschaffung der jünsten Systemsoftwareversion

Neueste allgemeine Version herunterladen:

- 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) Unter dem jeweiligen Modell auf den Link
- f) "Treiber & Downloads" klicken.
- g) Den Bildschirminhalt bis zum Bereich "Geräteaufrüstungen und -aktualisierungen" nach oben verschieben.
- h) Den Link mit Installationsanweisungen für Systemsoftwareversion xx.xx.xx.xxx anklicken und die Anleitung ausdrucken bzw. speichern.
- i) Den Link für die Aktualisierung der Systemsoftware auf Version xx.xx.xx.xxx 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 nach wichtigen Informationen zur Geräteaktualisierung durchsehen.
- l) Das Gerät aufrüsten.
- m) Zum Abschnitt "Patchinstallation" in diesem Dokument zurückkehren, auf den oben verwiesen wird.

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. Die Gesetzgebung mancher Länder verbietet den Haftungsausschluss bzw. die Haftungsbeschränkung bei Folgeschäden, so dass die vorgenannten Beschränkungen ggf. nicht zutreffend sind.