

XEROX-SICHERHEITSMERKBLATT XRX05-005

ESS/Netzwerkcontroller und MicroServer-Webserver sind anfällig für Command-Injection-Angriffe. Diese Sicherheitslücke kann zur Remoteausführung beliebiger Software missbraucht werden.

Patch P29 wird als Softwarelösung mit Installationsanweisungen für die unten genannten Produkte bereitgestellt. Dieses Korrekturprogramm ist vom Benutzer zu installieren. Bei der Patchinstallation zum Schutz vertraulicher Daten vor möglichen Angriffen über das Netzwerk wie nachfolgend beschrieben vorgehen.

Die Softwarelösung ist in einer ZIP-Datei mit 59 KB komprimiert und kann über diesen Link unter [Xerox.com/Security](http://www.xerox.com/Security) heruntergeladen werden:

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

Um die Sicherheitslücke für die u. g. Geräte zu schließen, sollte zunächst anhand der beigefügten Anweisungen geprüft werden, ob die Version der Systemsoftware mindestens SMP1 entspricht (Systemsoftwareversion 12.50.03.000, 13.50.03.000 oder 14.50.03.000 - je nachdem, ob es sich bei dem Gerät um ein WorkCentre® oder ein WorkCentre® Pro handelt). Falls eine ältere als Systemsoftwareversion *.50.03.000¹ installiert ist, kann letztere im Bereich "Treiber & Downloads" unter www.xerox.com heruntergeladen werden. Siehe Anhang A der Patchinstallationsanleitung zur Beschaffung der *.50.03.000-Systemsoftware.

Hinweis: Dieser Sicherheitspatch trägt die Bezeichnung **P29**. Nach der Patchinstallation enthält die Versionsangabe für den Netzwerkcontroller die BIOS-Version des Geräts und **.P29** (Z. B. 40.010.#1172.BIOS07.07.P29²)

Hintergrundinformation

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

- Command Injection über Webbenutzeroberfläche

Diese Sicherheitsanfälligkeit des ESS/Netzwerkcontrollers und Websservercodes erlaubt Angreifern u. U. die Umgehung der Authentifizierung und die Remoteausführung beliebiger Software.

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

Danksagung:

Xerox dankt

- Steve Puls, Rajat Mandal sowie Mike Webb für die Entwicklung und Prüfung dieses Korrekturprogramms.
- Brendan O'Connor für das Aufmerksammachen auf entsprechende Sicherheitslücken.

Geräte, auf die der Patch anwendbar ist:

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

Hinweis: Die Geräte WorkCentre® 7655/7665 sind von dieser Sicherheitslücke nicht betroffen.

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

² # entspricht 0, 1, oder 5, je nachdem, ob es sich bei dem Gerät um ein WorkCentre® oder ein WorkCentre® Pro handelt

Lösung

Installationshinweise

Name der Patchdatei: P29_WC2xx-Only_HTTP.dlm

Dieses Korrekturprogramm kann, wie nachfolgend beschrieben, ohne großen Aufwand in wenigen Minuten auf dem System installiert werden.

Versionen und erforderliche Handlungen:

	Softwareversion entspricht Systemsoftware oder Netzwerkcontroller		Patchinstallation möglich?	Nächster Schritt:	Dann:	Versionsangabe für Netzwerkcontroller/ESS jetzt wie folgt:
1	*.27.24.000 bis *.27.24.014	040.010.#0930 bis 040.010.#1110	Nein	Auf Version *.50.03.000 aktualisieren S. Hinweis 2 unten	Patch P29 anwenden	Aktualisieren, dann gemäß Reihe 3 fortfahren
2	*.27.24.016 bis *.27.24.020	040.010.#1120 bis 040.010.#1160	Ja	Patch P29 installieren	Fertig	040.010.#1120.BIOS07.07.P29 bis 040.010.#1160.BIOS07.07.P29
3	*.50.03.000 bis *.50.03.009	040.010.#1172 bis 040.010.#2250	Ja	Patch P29 installieren	Fertig	040.010.#1172.BIOS07.07.P29 bis 040.010.#2250.BIOS07.07.P29
4	*.50.03.011 oder höher	040.010.#2280 oder höher	Fehlerkorrektur in Version enthalten	Fertig	-	040.010.#2280 oder höher
5	*.27.24.015 nach Common Criteria zertifiziert	040.010.#1121	Ja	S. HINWEIS 1 unten	Fertig	040.010.#1120.BIOS07.07.P29
6	*.39.24.001 Nach Common Criteria zertifiziert	040.010.#1123	Ja	S. HINWEIS 1 unten	Fertig	040.010.#1123.BIOS07.07.P29

HINWEIS 1: Für Systemsoftwareversion *.27.24.015 oder *.39.24.001³ entspricht die Konfiguration der Zertifizierung nach den Common Criteria (Gemeinsame Kriterien für die Bewertung der Sicherheit von Informationstechnologie). Auf dem Gerät kann das Korrekturprogramm P29 installiert werden. Auf Wunsch kann Patch P29 geladen werden, die Zertifizierung des Geräts nach den Common Criteria geht damit jedoch verloren.

³ Netzwerkcontrollerversion 040.010.*1121 oder 040.010.*1123

Systemsoftwareversion ermitteln

Um herauszufinden, welche Version der Systemsoftware installiert ist, einen Konfigurationsbericht drucken oder die Version auf der Benutzeroberfläche des Webclients anzeigen.

Konfigurationsbericht über das Bedienfeld des Geräts ausgeben:

- 1) Systemstatustaste drücken.
- 2) Option zur Ausgabe des Konfigurationsberichts wählen.
- 3) "Konfigurationsbericht drucken" auswählen.
- 4) Versionsnummer der Systemsoftware suchen.

Version von der Webclient-Oberfläche anzeigen:

- 1) Webbrowser starten und durch Eingabe der IP-Adresse des Geräts die Verbindung zum Multifunktionsgerät herstellen.
- 2) Das Indexsymbol im oberen mittleren Fensterbereich auswählen.
- 3) "Konfiguration" auswählen.
- 4) Unter "Druckereinrichtung" wird die Version der Systemsoftware angezeigt.

HINWEIS 2: Falls die Systemsoftware nicht in einer der empfohlenen Versionen vorliegt, die Systemsoftwaredateien VOR der Patchinstallation gemäß den Anweisungen in Anhang A herunterladen, um die Software zu aktualisieren.

Patchinstallation

- 1) Webbrowser starten und durch Eingabe der IP-Adresse des Geräts die Verbindung zum Multifunktionsgerät herstellen.
- 2) Das Indexsymbol oben rechts im Fenster auswählen.
- 3) Die Option zur manuellen Aktualisierung auswählen.
- 4) Mit der "Durchsuchen"-Schaltfläche die Datei ansteuern und auswählen: **P29_WC2xx-Only_HTTP.dlm (Datei muss unkomprimiert sein (P29_WC2xx-Only_HTTP.ZIP.)**
- 5) "Software installieren" auswählen.
- 6) Benutzernamen (Admin) und das Administrator Kennwort für das Gerät eingeben.
- 7) Das WorkCentre wird zur Patchinstallation automatisch neu gestartet.
- 8) Das Korrekturprogramm ist installiert, wenn **.BIOSxx.yy.P29 (xx.yy steht für die BIOS-Version des Geräts)** an die Versionsnummer des Netzwerkcontrollers angehängt wurde.
Am WorkCentre selbst wird die Version nicht, sondern nur indirekt auf der Konfigurationswebseite angezeigt (sofern die Systemsoftware der Version *.50.03.000 oder höher entspricht).

Das Gerät wurde erfolgreich gepatcht.

Anhang A

Systemsoftwareversion *.50.03.000 beschaffen

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 *.50.03.000 anklicken und die Anleitung ausdrucken bzw. speichern.
- i) Den Link für die Aktualisierung der Systemsoftware auf Version *.50.03.000 anklicken und die Datei auf dem Computer speichern.
- j) Nach dem Herunterladen die Dateien in ein Verzeichnis auf dem Rechner extrahieren.
- k) Weitere Informationen zum Aufrüsten des Geräts enthält die Datei dc06cc0406.pdf, die im Downloadpaket enthalten ist.
- l) Die gespeicherten Anweisungen zur Systemsoftwareinstallation durchsehen.
- m) Das Gerät aufrüsten.
- n) Zum Abschnitt "Patchinstallation" in diesem Dokument zurückkehren.

<Ende der Anweisungen>

Haftungsausschluss

Die Informationen in dieser Xerox-Produktantwort 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 dieser Xerox-Produktantwort 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.