

XEROX-SICHERHEITSMERKBLATT XRX06-007

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. In diesem Bulletin wird die gleiche Sicherheitslücke behandelt wie in Sicherheitsbulletin XRX06-005, doch bezieht diese Version sich auf die unten genannten Produkte. Das 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 1 MB 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_WC-DC_Patches.zip

Hintergrund

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

- In der Webbenutzeroberfläche ist der TCP/IP-Hostname anfällig für Command-Injection-Angriffe

Diese Sicherheitsanfälligkeit des ESS/Netzwerkcontrollers und Webservercodes 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

- Brendan O'Connor für das Aufmerksammachen auf entsprechende Sicherheitslücken.

Dieses Korrekturprogramm gilt für vernetzte Versionen der folgenden Produkte:

Document Centre®	WorkCentre®	WorkCentre Pro®
220	M35	35
230	M45	45
240	M55	55
255	M165	65
265	M175	75
332		90
340		165
420		175
425		C32
426		C40
430		C2128
432		C2636
440		C3545
460		
470		
480		
490		
535		
545		
555		

Lösung

Vorgehensweise zur Installation des WebUI-Patches Bearbeitet am: 17. November 2006

Die Software von Patch 29 muss nur dann auf dem Multifunktionsgerät ausgeführt werden, wenn darauf eine der im Folgenden genannten Versionen der Systemsoftware installiert ist. Es stehen 3 separate Korrekturprogramme zur Verfügung, die für jeweils unterschiedliche Gruppen von Multifunktionsgeräten bestimmt sind.

Die Patches müssen heruntergeladen werden. Sie sind im ZIP-Format komprimiert. Die ZIP-Datei vom angegebenen URL herunterladen und den gesamten Inhalt auf die Festplatte eines PCs extrahieren. NICHT VERSUCHEN, DIE DATEI MIT DER ERWEITERUNG .TGZ ZU ÖFFNEN. Die Patchdateien dürfen in keiner Weise verändert werden.

Ausführliche Anweisungen zum Beseitigen der Sicherheitslücke auf Document Centre-/ WorkCentre Pro-Geräten sind zu finden 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>.

Anweisungen für das Xerox WorkCentre M35/M45/M55 - M165/M175 und Xerox WorkCentre Pro 35/45/55 - 65/75/90 und das Xerox WorkCentre Pro C32/40, WCP C2128/C2636/C3545 - Patch P29

Name der Patch-Datei: **P29-WC_WCPModels.tgz**

Erforderlich für folgende Softwareversionen: **WCP**

	Systemsoftware	Net-Controller/ESS
WC M35/M45/M55	2.28.11.000 bis 2.97.20.076	1.02.129.1 bis 1.08.129.1
WCP 35/45/55	3.28.11.000 bis 3.97.20.076	1.02.329.1 bis 1.08.329.1
WC M35/M45/M55 mitPS-Option	4.28.11.000 bis 4.97.20.076	1.02.229.1 bis 1.02.229.1
WCP 65/75/90	1.001.00.060 bis 1.001.02.722	1.00.60.3 bis 1.08.022.01
WC M165/M175	6.47.39.000 bis 6.57.33.017	1.03.464.2 bis 1.03.482.1
WCP 165/175	7.47.39.000 bis 7.57.33.017	1.03.664.2 bis 1.03.682.1
WC M165/M175 mit PS-Option	8.47.30.000 bis 8.57.33.017	1.03.564.2 bis 1.03.582.1
WCP C32/C40	1.001.00.060 bis 1.001.02.723	1.00.60.3 bis 1.08.023.01
WCP C2128/C2636/C3545	1.001.04.044 bis 0.001.4.519	3.04.044.01 bis 3.04.519.02

HINWEIS: Ist auf dem Gerät eine höhere Version der Systemsoftware oder des Net-Controllers/ESS installiert, braucht der Patch nicht installiert zu werden.

Bestätigung der Systemsoftware-Version

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

Ausdrucken eines Konfigurationsberichts über die lokale Benutzeroberfläche am Gerät:

- 1) Systemstatustaste drücken
- 2) Option zur Ausgabe des Konfigurationsberichts auswählen
- 3) Versionsnummer der Systemsoftware suchen.

Anzeigen der Version von der Web-Client-Oberfläche:

- 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.
- 4) "Konfiguration" auswählen.

- 5) Zur Position "Druckereinrichtung" scrollen, an der die Version der Systemsoftware angezeigt wird.

Installation des Patches

NICHT VERSUCHEN, DEN PATCH ZU ÖFFNEN. DIE DATEI KANN DADURCH BESCHÄDIGT WERDEN. Für die Patchübermittlung an dieses Modell stehen drei Methoden zur Verfügung.

- 1) LPR-Methode für alle WCPs
- 2) Geräte-Software-Methode (Aktualisierung) für alle WCPs
- 3) CentreWare-Web. Ausführliche Hinweise sind über den oben angegebenen Kundentipp-Link erhältlich.

LPR-Methode von einem PC mit Windows NT, 2000 oder XP

Um diese Methode verwenden zu können, muss das LPR-Protokoll auf dem Gerät aktiviert sein. Im Konfigurationsbericht nachsehen, ob das Protokoll aktiviert ist. Dieses Protokoll kann über die lokale Benutzeroberfläche oder über die Web-Oberfläche aktiviert werden. Anweisungen hierzu befinden sich in Anhang A.

- 1) Eine DOS-Befehlsaufforderung öffnen. Dazu das Windows-Startmenü und anschließend "Ausführen" auswählen.
- 2) "cmd" eingeben und die Eingabetaste drücken.
- 3) Die Patch-Datei mit folgender Befehlszeile übermitteln: **lpr -S <drucker_ip> -Plp P29_WC_WCPModels.tgz**

Auf allen WCPs wird ein Patchinstallationsblatt ausgedruckt und automatisch ein Neustart durchgeführt, um den Patch zu installieren. Der Patch ist installiert, wenn an die Versionsnummer des Netzwerkcontrollers **.P29** angehängt wurde. Bei der WorkCentre M-Serie (M35, M45, M55, M165, M175) wird **.P29** NICHT angehängt, obwohl der Patch installiert ist. Die erfolgte Installation kann auch mithilfe der Systemsoftware- oder der Netzwerk-Controller-/ESS-Version überprüft werden.

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) Benutzernamen und Kennwort des Geräts eingeben.
- 5) Unter "Manuelle Aktualisierung" die Schaltfläche "Durchsuchen" und anschließend die Datei **P29_WC_WCPModels.tgz** auswählen.
- 6) "Software installieren" auswählen.
- 7) Auf allen WCPs wird ein Patchinstallationsblatt ausgedruckt und automatisch ein Neustart durchgeführt, um den Patch zu installieren. Der Patch ist installiert, wenn an die Versionsnummer des Netzwerkcontrollers **.P29** angehängt wurde. Bei der WorkCentre M-Serie (M35, M45, M55, M165, M175) wird **.P29** NICHT angehängt, obwohl der Patch installiert ist.

Anweisungen für das Document Centre 535/545/555 Patch P29

Anweisungen für das Document Centre 240/255/265/460/470/480/490 Patch P29

Anweisungen für das Document Centre 420/425/426/430/432/440 Patch P29

Name der Patch-Datei: **P29-DC555f-440F-490f-265f.tgz**

Erforderlich für folgende Softwareversionen: **Document Centre**

	Systemsoftware	Net-Controller/ESS
DC 535/545/555	14.52.000 bis 27.18.036	0.19.10.047.1 - 19.12.029.1
DC 460/470/480/490	19.5.026 bis 19.5.535	07.19.05.026 bis 07.19.05.535
DC 420/426/432/440*	Nicht zutreffend	2.3.0.2 bis 2.3.26
DC 425/432/440	Nicht zutreffend	3.0.5.4 bis 3.2.47
DC 430	Nicht zutreffend	3.3.24 bis 3.3.47
DC 240/255/265	6.03 bis 6.32	0.18.1.24 bis 0.18.6.82

***Hinweise zu Versionen vor 2.2.18 sind dem folgenden Abschnitt zu entnehmen**

HINWEIS: Ist auf dem Gerät eine höhere Version der Systemsoftware oder des Net-Controllers/ESS installiert, braucht der Patch nicht installiert zu werden.

Bestätigung der Systemsoftware-Version

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

Ausdrucken eines Konfigurationsberichts von der lokalen Benutzeroberfläche am Gerät:

- 1) Systemstatustaste drücken
- 2) Option zur Ausgabe des Konfigurationsberichts auswählen
- 3) Versionsnummer der Systemsoftware suchen.

Anzeigen der Version von der Web-Client-Oberfläche:

- 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) "Konfiguration" auswählen.
- 4) Zur Position "Druckereinrichtung" scrollen, an der die Version der Systemsoftware angezeigt wird.

Installation des Patches

NICHT VERSUCHEN, DEN PATCH ZU ÖFFNEN. DIE DATEI KANN DADURCH BESCHÄDIGT WERDEN.
Für die Patchübermittlung an dieses Modell stehen zwei Methoden zur Verfügung.

- 1) LPR-Methode für alle DCs
- 2) Geräte-Software-Methode (Aktualisierung) nur für DC 460/470/480/490 535/545/555 und DC 240/255/265.

LPR-Methode von einem PC mit Windows NT, 2000 oder XP

Um diese Methode verwenden zu können, muss das LPR-Protokoll auf dem Gerät aktiviert sein. Im Konfigurationsbericht nachsehen, ob das Protokoll aktiviert ist. Dieses Protokoll kann über die lokale Benutzeroberfläche oder über die Web-Oberfläche aktiviert werden. Anweisungen hierzu befinden sich in Anhang A.

- 1) Eine DOS-Befehlsaufforderung öffnen. Dazu das Windows-Startmenü und anschließend "Ausführen" auswählen. "cmd" eingeben und die Eingabetaste drücken.
- 2) Die Patch-Datei mit folgender Befehlszeile übermitteln: **lpr -S <drucker_ip> -Plp P29_DC555f-440F-490f-265f.tgz**
- 3) Das Document Centre 535/545/555 und das Document Centre 240/255/265/460/470/480/490 wird automatisch neu gestartet, um den Patch zu installieren. Bei erfolgreicher Patchinstallation wird die Versionsnummer des Netzwerkcontrollers durch die Angabe **.P29** erweitert.

- 4) Bei den Document Centre-Modellen 420/426/430/432/440 muss entweder ein Remote-Reset durchgeführt oder das Gerät aus- und wieder eingeschaltet werden, um den Patch zu installieren.

HINWEIS: Nach dem automatischen Neustart muss auf dem Document Centre 240/255/265/460/470/480/490 eine zweite Konfigurationsseite ausgedruckt werden, um den Patch **.P29** an die Netzwerk-Controllerversion zu übermitteln.

Geräte-Software-Methode (Aktualisierung)

Diese Methode gilt nur für die Produkte DC535/545/555, DC490/480/470/460 und DC240/255/265.

- 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) Benutzernamen und Kennwort des Geräts eingeben.
- 5) Unter "Manuelle Aktualisierung" die Schaltfläche "Durchsuchen" und anschließend die Datei **P29_DC555f-440F-490f-265f.tgz** auswählen.
- 6) "Software installieren" auswählen.

Das Document Centre 535/545/555 und das Document Centre 240/255/265/460/470/480/490 wird automatisch neu gestartet, um den Patch zu installieren. Bei erfolgreicher Patchinstallation wird die Versionsnummer des Netzwerkcontrollers durch die Angabe **.P29** erweitert.

HINWEIS: Nach dem automatischen Neustart muss möglicherweise eine Konfigurationsseite manuell gedruckt werden, um zu prüfen, ob **.P29** an die Version des Net-Controllers angehängt wurde.

Anweisungen für das Document Centre 220/230/332/340 Patch P29

Name der Patch-Datei: **P29-DC220f-332f-420launch.dlm**

Erforderlich für folgende Softwareversionen: **DC**

	Systemsoftware	Net-Controller/ESS
DC 220/230/332/340		1.12.35.1 bis 1.12.87
DC 425/432/440*		2.1.2 bis 2.2.18

***Hinweise zu Versionen vor 2.2.18 sind dem folgenden Abschnitt zu entnehmen**

	Systemsoftware	ESS
DC 220/230/332/340	Nicht zutreffend	1.12.35.1 bis 1.12.87
DC 425/432/440*	Nicht zutreffend	2.1.2 bis 2.2.18

HINWEIS: Ist auf dem Gerät eine höhere ESS-Version installiert, muss der Patch nicht installiert werden.

Bestätigung der Version der ESS-Software

Um herauszufinden, welche Version der ESS-Software installiert ist, kann entweder ein Konfigurationsbericht gedruckt oder die Version auf der Web-Client-Benutzeroberfläche angezeigt werden.

Ausdrucken eines Konfigurationsberichts von der lokalen Benutzeroberfläche am Gerät:

- 1) Systemstatustaste drücken
- 2) Option zur Ausgabe des Konfigurationsberichts auswählen
- 3) Versionsnummer der ESS-Software suchen

Anzeigen der Version von der Web-Client-Oberfläche:

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen.
- 2) Das Geräteindexsymbol im oberen Bereich des Bildschirms in der Mitte auswählen.
- 3) **Gerätekonfiguration** auswählen.
- 4) Zur Stelle scrollen, an der die Version der ESS-Software angezeigt wird.

Installation des Patches

NICHT VERSUCHEN, DEN PATCH ZU ÖFFNEN. DIE DATEI KANN DADURCH BESCHÄDIGT WERDEN.

LPR-Methode von einem PC mit Windows NT, 2000 oder XP

Um diese Methode verwenden zu können, muss das LPD-Protokoll auf dem Gerät aktiviert sein. Im Konfigurationsbericht nachsehen, ob das LPD-Protokoll aktiviert ist. Dieses Protokoll kann über die lokale Benutzeroberfläche oder über die Web-Oberfläche aktiviert werden. Anweisungen hierzu befinden sich in Anhang A.

- 1) Eine DOS-Befehlsaufforderung öffnen. Dazu das Windows-Startmenü und anschließend "Ausführen" auswählen. "cmd" eingeben und die Eingabetaste drücken.
- 2) Die Patch-Datei mit folgender Befehlszeile übermitteln: **lpr -S <drucker_ip> -Plp P29_DC220f-332f-420launch.dlm**
- 3) Gerät aus- und wieder einschalten. Warten, bis das Gerät neu gestartet wird.
- 4) **Gerät nochmals aus- und wieder einschalten** .
- 5) Der Patch ist installiert, wenn an die ESS-Versionsnummer **.P29** angehängt wurde.

Anhang A – Aktivierung von LPD, Drucken über Anschluss 515

Um den Patch mit der LPR-Methode senden zu können, muss das Multifunktionsgerät LPD (Line Printer Daemon) über Anschluss 515 unterstützen. Bei den meisten Multifunktionsgeräten ist diese Option standardmäßig aktiviert. Falls der LPD-Druck deaktiviert wurde, muss er jetzt wieder aktiviert werden, um die LPR-Methode verwenden zu können.

Zum Aktivieren von LPD auf den Document Centre-Modellen 240/255/265/420/425/432/440/460/470/480/490/535/545/555 sowie den WorkCentre-/WorkCentre Pro-Modellen wie folgt vorgehen:

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen
- 2) Das Symbol "Index" im oberen Bereich des Bildschirms auswählen.
- 3) "LPR/LPD" oder "Line Printer Daemon" auswählen
- 4) Ist das Feld "Aktiviert" NICHT aktiviert, das Feld auswählen, um es zu aktivieren.
- 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.

Zum Aktivieren von LPD auf dem Document Centre 220/230/332/340 wie folgt vorgehen:

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen
- 2) Das Symbol "Index" oben rechts auswählen
- 3) "Protokolle" auswählen, zu "LPD" scrollen und den Link "LPD" auswählen.
- 4) Ist das Feld "Aktiviert" NICHT aktiviert, das Feld auswählen, um es zu aktivieren.
- 5) "Anwenden" auswählen
- 6) Benutzernamen Admin und Admin-Kennwort eingeben und "OK" auswählen.
- 7) Multifunktionsgerät aus- und wieder einschalten.

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 Marktauglichkeit 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.