

27.06.2005

## **XEROX SICHERHEITSBULLETIN XRX05-006**

Aufgrund von Schwachstellen im Xerox MicroServer-Webserver ist ein Zugriff durch unbefugte Personen nicht ausgeschlossen.

Die folgende Softwarelösung und die nachstehend beschriebenen Installationsanweisungen werden für die aufgelisteten Produkte zur Verfügung gestellt, um Ihre vertraulichen Daten vor möglichen Angriffen über das Netzwerk zu schützen.

Die Softwarelösung ist in einer Zip-Datei (581 KB) komprimiert und kann über den Link in diesem Bulletin unter [www.xerox.com / security](http://www.xerox.com/security) heruntergeladen werden:

[http://www.xerox.com/downloads/usa/en/c/cert\\_P22\\_NIAP\\_WCP\\_C\\_Only.zip](http://www.xerox.com/downloads/usa/en/c/cert_P22_NIAP_WCP_C_Only.zip)

### **Hintergrund**

Im Webserver-Code befinden sich mehrere Schwachstellen, über die ein unberechtigter Zugriff auf den Webserver möglich ist. Diese Schwachstellen umfassen:

- Schwachstellen, die eine Authentifizierung umgehen könnten.
- Speziell konstruierte HTTP-Anweisungen, die zu einem DoS (Denial of Service) oder einem unerlaubten Dateizugriff auf einem angegriffenen Gerät führen könnten.
- Cross-Site-Scripting (Angriffe auf Webservices über das HTTP-Protokoll), durch die Inhalte von Webseiten unerlaubt geändert werden können.

Wenn es einem Angreifer gelingt, auf den Webserver zuzugreifen, könnte er unberechtigte Änderungen an der Systemkonfiguration vornehmen. Kennwörter von Kunden und Benutzern sind nicht gefährdet.

**Hinweis: Dieser Patch wird nur für die nachstehend aufgeführten Produkte benötigt.**

### **Betroffene Produkte:**

#### **WorkCentre® Pro**

C2128  
C2636  
C3545

27.06.2005

## Lösung

### Patch für MicroServer-Webserver Bearbeitet am: 21. Juni 2005

Mit dem vorliegenden Patch werden Schwachstellen im Xerox MicroServer-Webserver beseitigt, die bei den WorkCentre-Multifunktionsgeräten C2128/2636/3545 aufgedeckt wurden. Die Patch-Software muss nur dann auf dem Multifunktionsgerät ausgeführt werden, wenn auf dem Multifunktionsgerät eine der im Folgenden aufgeführten Versionen der Systemsoftware installiert ist.

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 .TGZ ZU ÖFFNEN. Diese Datei ist der Patch, der im unveränderten Zustand auf das Multifunktionsgerät geladen werden muss.

### Installationsanweisungen

Name der Patch-Datei: **P22\_niap\_wcp\_c.tgz**

Dieser Patch wird nur benötigt, wenn auf dem WorkCentre eine der folgenden Versionen der Systemsoftware installiert ist:

**WorkCentre Pro Color 2128/2636/3545 Version 0.001.04.044 bis 0.001.04.505**

**Ist auf dem Gerät eine höhere Version der Systemsoftware installiert, braucht der Patch nicht installiert zu werden.**

### **Bestätigung der Version der Systemsoftware**

Um herauszufinden, welche Version der Systemsoftware 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 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. Der Patch kann auf zwei Arten an dieses Modell gesendet werden.

- 1) LPR-Methode
- 2) Geräte-Software-Methode (Aktualisierung)

### **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.

27.06.2005

- 2) Die Patch-Datei mit folgender Befehlszeile senden: **lpr -S <drucker\_ip> -Plp P22\_NIAP\_WCP\_C Only.tgz**
- 3) Das WorkCentre wird automatisch neu gestartet, um den Patch zu installieren.
- 4) Der Patch ist installiert, wenn an die Versionsnummer des Netzwerkcontrollers **.P22** angehängt wurde.

27.06.2005

## 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 (Admin) und das Administrator-Kennwort des Geräts eingeben.
- 5) Unter "Manuelle Aktualisierung" die Schaltfläche "Durchsuchen" und anschließend die Datei **P22\_NIAP\_WCP\_C Only.tgz** auswählen.
- 6) "Software installieren" auswählen.
- 7) Das WorkCentre wird automatisch neu gestartet, um den Patch zu installieren.
- 8) Der Patch ist installiert, wenn an die Versionsnummer des Netzwerkcontrollers **.P22** angehängt wurde.

## 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 ggf. nicht auf Sie zutreffen.