

10.8.2005

XEROX SICHERHEITSBULLETIN XRX05-009

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

Die folgende Softwarelösung und die in diesem Dokument enthaltenen Installationsanweisungen werden für die aufgelisteten Produkte bereitgestellt, damit Sie Ihre vertraulichen Daten vor möglichen Angriffen über das Netzwerk schützen können.

Die Softwarelösung ist in einer Zip-Datei komprimiert (deren Größe in MB bisher noch nicht feststeht) und kann über den Link in diesem Bulletin unter Xerox.com / Security heruntergeladen werden:

http://www.xerox.com/downloads/usa/en/c/cert_P24-25_MicroServer_Web_Server_Patches.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.

Dieser Patch ist ein kumulativer Patch für die nachstehend aufgelisteten Produkte, der den Sicherheitspatch enthält, der im Sicherheitsbulletin XRX04-002 (P4) dokumentiert wurde.

Betroffene Produkte:

Document Centre®

220
230
332
340

10.8.2005

Lösung

Vorgehensweise zur Installation des WebUI-Patches

Bearbeitet am: 9.8.2005

Mit dem vorliegenden Patch werden Schwachstellen im Xerox MicroServer-Webserver beseitigt, die bei Document Centre-Multifunktionsgeräten 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. Dieser Patch ersetzt den früheren Patch P4.

Der Patch ist im ZIP-Format komprimiert. Die ZIP-Datei vom angegebenen URL herunterladen und den gesamten Inhalt auf den Desktop extrahieren. Der Patch muss wie im Folgenden beschrieben auf den Geräten installiert werden. Den Patch so wie er ist an die Geräte senden – nicht die Dateien öffnen.

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

Name der Patch-Datei: **P25_http_DC220-340.dlm**Erforderlich für ESS-Version: **1.12.08 bis 1.12.85****Ist auf dem Gerät ESS-Version 1.12.87 oder höher installiert, wird der Patch nicht benötigt.**

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 Position 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 senden: **lpr -S <drucker_ip> -P lp P25_http_DC220-340.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 **.P25** angehängt wurde

HINWEIS: Wenn P25 nicht an die ESS-Versionsnummer angehängt wurde, an das Kunden-Support-Zentrum wenden, damit die ESS-Version auf dem Gerät auf Version 1.12.85 bzw. auf das neueste verfügbare Release aktualisiert wird.

10.8.2005

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.

Die folgenden Schritte ausführen, um LPD zu aktivieren:

- 1) Einen Webbrowser öffnen und durch Eingabe der IP-Adresse des Geräts eine Verbindung zum Multifunktionsgerät herstellen
- 2) Das Geräteindexsymbol 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) Als Benutzernamen Admin, dann das Administratorkennwort 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. Einige Staaten/Länder verbieten den Ausschluss oder die Beschränkung der Haftung für Folgeschäden, so dass diese Beschränkungen ggf. nicht auf Sie zutreffen.