

Xerox Sicherheitsbulletin XRX08-004

Softwareupdate zur Behebung einer Cross-Site-Scripting-Schwachstelle

Version 1.0
22.05.2008

Hintergrund

Im Webserver der nachstehend aufgeführten Produkte besteht eine persistente Cross-Site-Scripting-Schwachstelle. Angreifer könnten diese Schwachstelle dazu ausnutzen, beliebigen Code in die von anderen Benutzern betrachteten Webseiten einzufügen. Kunden- und Benutzerkennwörter sind jedoch nicht gefährdet.

Wir wurden von Louhi Networks aus Finnland über diese Schwachstelle informiert. Außer dem Proof-of-Concept-Code, der vom Sicherheitsforscher zur Verfügung gestellt wurde, ist Xerox kein anderer Exploit-Code bekannt.

Xerox stellt den Schutz seiner Kunden an oberste Stelle und stellt darum für die unten aufgeführten Produkte ausführbare¹ oder binäre Dateien mit den Netzwerkcontroller-Software-Releases zur Verfügung, die diese Schwachstelle beheben. Diese Lösungen sind vom Kunden zu installieren. Zur Installation der Lösungen zum Schutz Ihres Produkts vor möglichen Angriffen über das Netzwerk wie nachfolgend beschrieben vorgehen.

Die Softwarelösungen sind produktspezifisch in einer von sechs ausführbaren Dateien komprimiert und sind über die nachstehenden Links oder über die Links am Ende dieses Bulletins unter <http://www.xerox.com/security> herunterladbar:

- WorkCentre 7132 Standarddatei (.EXE): http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-STD_EXEC.zip
- WorkCentre 7132 Standarddatei (Binär): http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-STD_BIN.zip
- WorkCentre 7132 mit Postscript-Datei (.EXE): http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-PS_EXEC.zip
- WorkCentre 7132 mit Postscript-Datei (Binär): http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7132-PS_BIN.zip
- WorkCentre 7228/7235/7245 EXE-Datei: http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7228-7235-7245_EXEC.zip
- WorkCentre 7228/7235/7245 Binärdatei: http://www.xerox.com/downloads/usa/en/c/cert_P35_WC7228-7235-7245_BIN.zip

Diese Lösungen sind als ein **kritischer** Patch eingestuft.

Danksagung

Xerox möchte sich bei Henri Lindberg, Louhi Networks, Finnland (www.louhi.fi) bedanken, der uns zuerst auf diese Schwachstelle hingewiesen hat.

Diese Softwarelösung bezieht sich auf vernetzte Versionen² der folgenden Produkte:

WorkCentre®
7132
7228
7235
7245

¹Firmware-Update-Tool für Windows: ein Firmware-Update-Tool, das mit dem Software-Release gebündelt ist und es Kunden ermöglicht, das Software-Release selbst zu installieren

²Wenn das Gerät nicht an ein Netzwerk angeschlossen ist, besteht keine Gefahr und es brauchen folglich auch keine Maßnahmen getroffen zu werden.

Lösung

Vorgehensweise zur Installation des Patches

Bearbeitet am: 19.05.2008

Installationsanweisungen

Patch-Dateiname für WC 7228/7235/7245:

- cert P35 WC7228 7235 7245 EXEC.zip (selbstextrahierende ausführbare Datei)
- cert P35 WC7228 7235 7245 BIN.zip (Binärdatei zur Verwendung mit Centreware Web)

Patch-Dateiname für WC 7132:

- cert P35 WC7132-STD EXEC.zip (STD-Version der selbstextrahierenden ausführbaren Datei)
- cert P35 WC7132-STD BIN.zip (STD-Version der Binärdatei zur Verwendung mit Centreware Web)
- cert P35 WC7132-PS EXEC.zip (PS-Version der selbstextrahierenden ausführbaren Datei)
- cert P35 WC7132-PS BIN.zip (PS-Version der Binärdatei zur Verwendung mit Centreware Web)

Für PS-Version des WC 7132 cert P35 WC7132-PS EXEC.zip oder cert P35 WC7132-PS BIN.zip verwenden

Für STD-Version des WC 7132 cert P35 WC7132-STD EXEC.zip oder cert P35 WC7132-STD BIN.zip verwenden

	Softwareversion entspricht Controller-ROM	Patchinstallation möglich?	Nächster Schritt:	Dann:	Versionsangabe für Controller-ROM jetzt wie folgt:
1	1.202.1 bis unter 1.202.6	Ja	Patch laden (für WC 7132 siehe Hinweise 1 und 2 unten)	-	1.202.6

HINWEIS 1 für WC 7132: Beim WC 7132 muss zuerst ermittelt werden, welche Datei auf das Gerät geladen werden muss. Das WC 7132 kann als eine PS- oder eine STD-Version konfiguriert werden. Näheres hierzu siehe Anhang A unten.

HINWEIS 2 für WC 7132: cert P35 WC7132-STD EXEC.zip und cert P35 WC7132-PS EXEC.zip sind selbstextrahierende ausführbare Dateien. Beide ausführbaren Dateien verwenden das in Anhang B unten beschriebene Firmware-Update-Tool. Eine Installation von CentreWare Web aus ist für dieses Produkt nicht möglich. Wenn CentreWare Web verwendet wird, nicht die .EXE-Datei, sondern die Datei cert P35 WC7132-STD BIN.zip oder cert P35 WC7132-PS BIN.zip verwenden.

Für WC 7228/7235/7245 WC7228 7235 7245 EXEC.zip oder cert P35 WC7228 7235 7245 BIN.zip verwenden (siehe Hinweis 1 unten für WC 7228/7235/7245)

	Softwareversion entspricht Controller-ROM	Patchinstallation möglich?	Nächster Schritt:	Dann:	Versionsangabe für Controller-ROM jetzt wie folgt:
1	1.220.0 bis unter 1.221.9	Ja	Patch laden (für WC 7228/7235/7245 siehe Hinweis 1 unten)	-	1.221.9

HINWEIS 1 für WC 7228/7235/7245: cert P35 WC7228 7235 7245 EXEC.zip ist eine selbstaufzuführende Datei, die das in Anhang B unten beschriebene Firmware-Update-Tool verwendet. Wenn CentreWare Web verwendet wird, nicht die .EXE-Datei, sondern die Datei cert P35 WC7228 7235 7245 BIN.zip verwenden.

Installation des Patches

Der Patch muss heruntergeladen werden. Der Patch ist im ZIP-Format komprimiert. Die ZIP-Datei von der angegebenen URL herunterladen und den gesamten Inhalt auf den Desktop extrahieren. Nicht versuchen, die Datei mit der Erweiterung .DLM zu öffnen. Diese Datei ist der Patch, der im unveränderten Zustand auf das Multifunktionsgerät geladen werden muss.

Vorgehensweisen für die Patchinstallation

Dieser Patch und die Aktualisierungssoftware sollten (wie Software i. A.) nach Möglichkeit vom Kunden installiert werden.

Die Installation kann auf verschiedene Weisen erfolgen.

- Die selbstextrahierende ausführbare Datei verwenden, die das Firmware-Update-Tool nutzt. Siehe Anhang B.
- XDM/Centreware Web zum Senden von Aktualisierungs-/Patchdateien an mehrere Geräte verwenden. Weitere Informationen zu dieser Methode befinden sich 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>

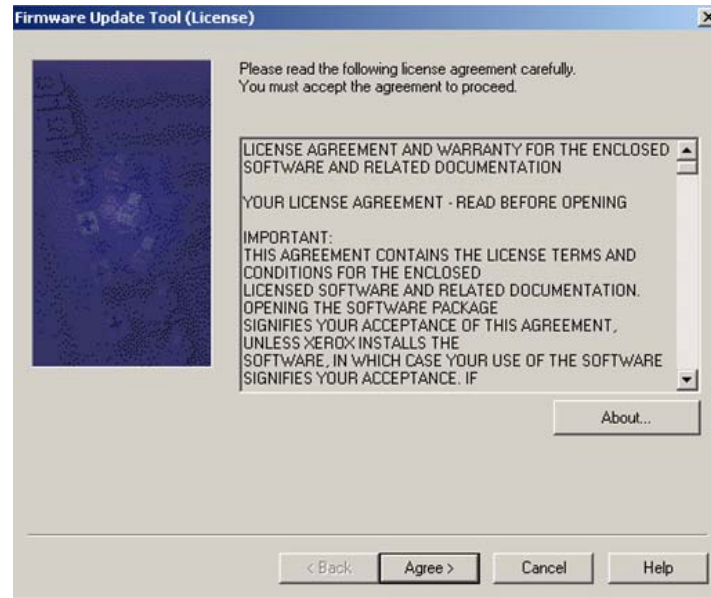
Anhang A: Ermittlung, ob das WC 7132 als PS oder STD konfiguriert ist:

Es ist wichtig, dass zur Aktualisierung Ihres Geräts die richtige Aktualisierungsdatei verwendet wird. Die momentan auf dem Gerät ausgeführte Softwareversion wie folgt ermitteln:

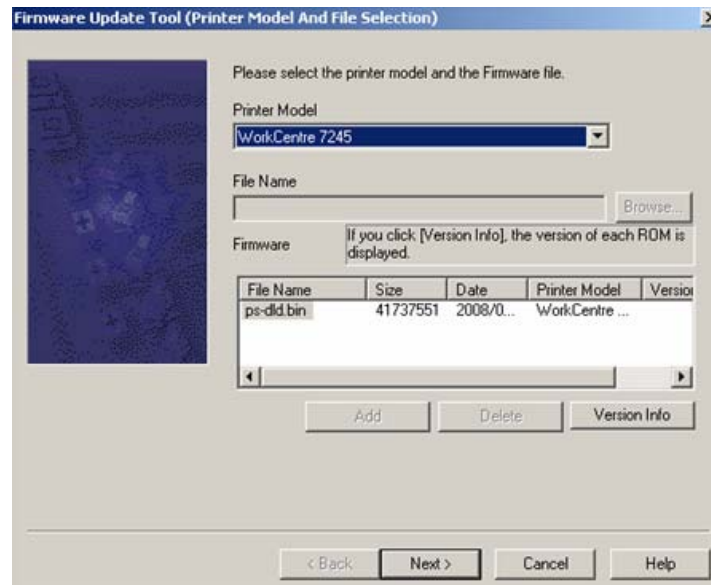
1. Webbrowser öffnen und in das Adressfeld <http://> gefolgt von der TCP/IP-Adresse des Geräts eingeben und dann die Eingabetaste drücken.
2. Auf die Registerkarte „Einstellung“ klicken.
3. Auf „Konfiguration“ klicken.
4. Einen Bildlauf nach unten zum Softwareabschnitt durchführen, um die Version des Controllers zu sehen. Nachsehen, oder der Controller-ROM als Controller-ROM oder als Controller+PS ROM aufgeführt ist. Hiervon hängt ab, welche Datei von Xerox.com heruntergeladen werden muss. Für den Controller-ROM muss die STD-Datei geladen werden. Für den Controller+PS ROM muss die PS-Datei geladen werden.

Anhang B: Verwendung des Firmware-Update-Tools (selbstextrahierende .EXE-Datei):

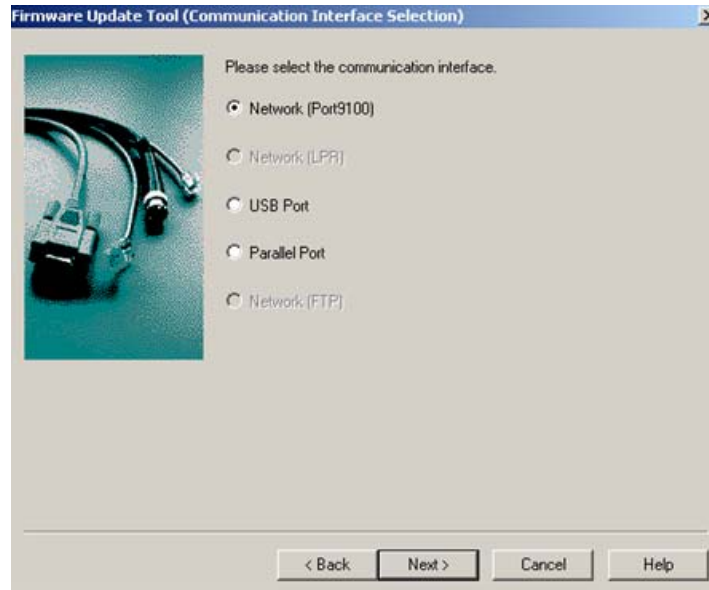
1. Das Firmware-Update-Tool kann nur unter Windows-Betriebssystemen eingesetzt werden. Bei anderen Betriebssystemen den Xerox-Kundendienst kontaktieren, um den Patch von einem Kundendiensttechniker laden zu lassen.
2. Das Firmware-Update-Tool verwendet Anschluss 9100. Anschluss 9100 ggf. auf dem Gerät aktivieren, damit das Tool verwendet werden kann. Vorgehensweise:
 - a. Webbrowser öffnen und in das Adressfeld <http://> gefolgt von der TCP/IP-Adresse des Geräts eingeben. Eingabetaste drücken.
 - b. Auf die Registerkarte „Einstellung“ klicken.
 - c. Auf „Anschlusstatus“ klicken.
 - d. Nachsehen, ob das Kontrollkästchen neben „Anschluss 9100“ aktiviert ist. Wenn nicht, das Kontrollkästchen aktivieren und dann unten auf der Webseite auf „Übernehmen“ klicken.
3. Sich vergewissern, dass das Gerät von niemandem benutzt wird, dann mit der Aktualisierung fortfahren. Mit „dass das Gerät von niemandem benutzt wird“ ist gemeint, dass gerade keine Aufträge vom Gerät verarbeitet werden und dass keine Aufträge direkt am Gerät programmiert werden.
4. Auf die .EXE-Datei doppelklicken. Das unten gezeigte Dialogfeld erscheint. Den Lizenzvertrag lesen und ihm durch einen Klick auf die entsprechende Schaltfläche zustimmen, um mit der Installation fortzufahren. Bei der Aktualisierung eines WC 7132 darauf achten, dass die richtige Datei (PS oder STD) gewählt wurde (siehe Anweisungen in Anhang A oben).



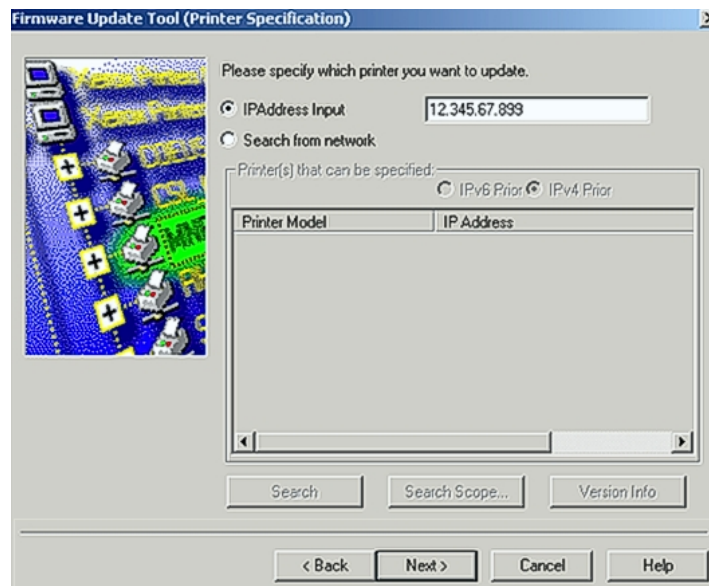
5. Im nächsten Dialogfeld aus der Dropdownliste das jeweilige Druckermodell auswählen. Für WC 7228/7235/7245 stehen folgende Modelle zur Auswahl: WorkCentre 7228, WorkCentre 7235, WorkCentre 7245. Das richtige Modell auswählen. Für WC 7132 steht nur das WorkCentre 7132 zur Auswahl.



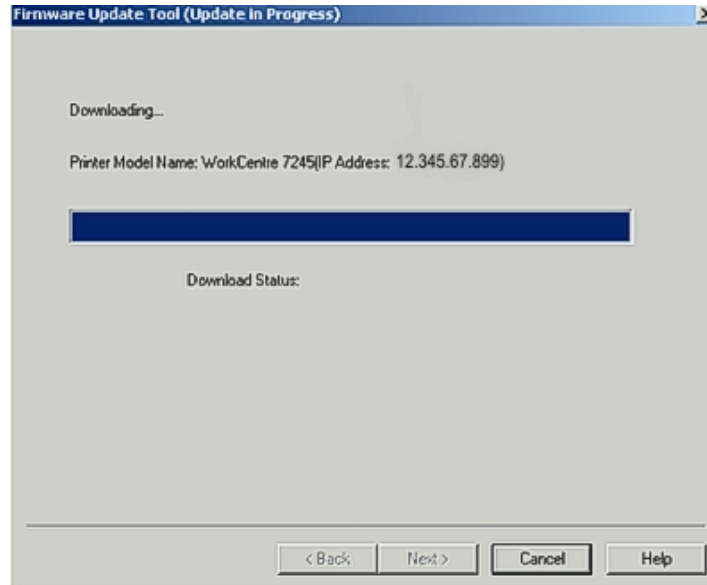
6. „Network (Port9100)“ (Netzwerk (Anschluss9100)) auswählen (sofern diese Option noch nicht ausgewählt ist) und auf „Next“ (Weiter) klicken.



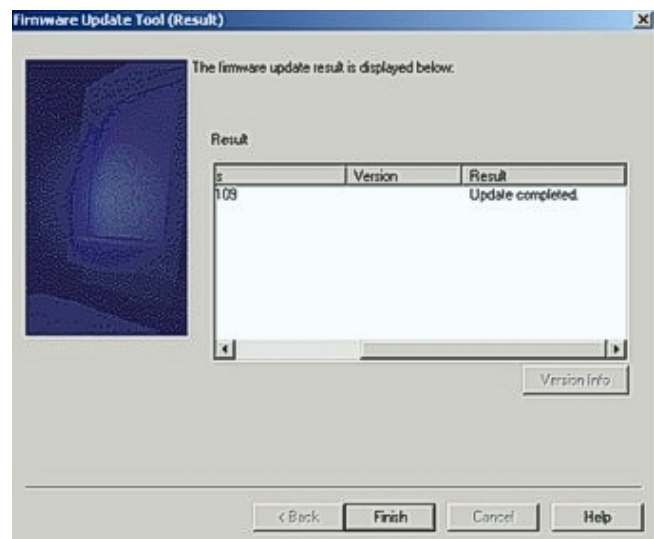
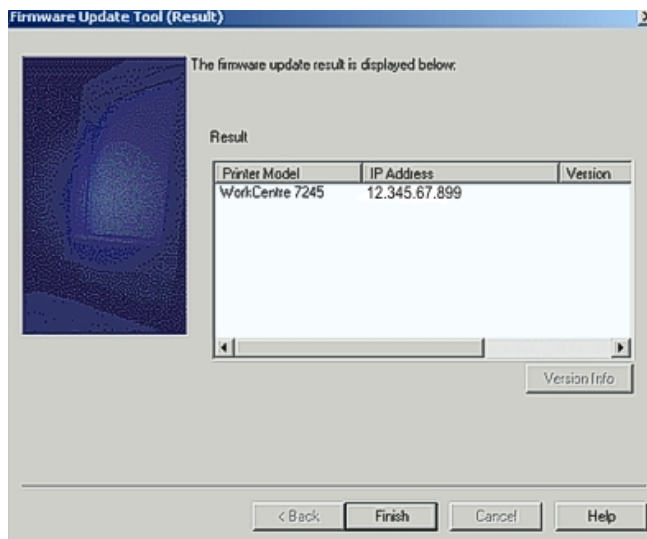
7. „IPAddress Input“ (IP-Adresse eingeben) auswählen und die TCP/IP-Adresse des Geräts eingeben. Auf „Next“ (Weiter) klicken. Wenn in Schritt 5 oben das falsche Druckermodell gewählt wurde und in diesem Dialogfeld auf „Next“ (Weiter) geklickt wird, kann der Aktualisierungsprozess nicht fortgesetzt werden.



8. Der Patch wird auf das Gerät geladen. Dieser Vorgang dauert etwa 10-15 Minuten.



9. Warten, bis das Dialogfeld „Firmware Update Result is Displayed Below“ (Firmware-Update-Ergebnis ist unten angezeigt) erscheint (bis dahin auf keine Schaltflächen im Firmware-Update-Tool klicken). Den Status der Aktualisierung prüfen. Hierzu einen Bildlauf nach rechts durchführen und nachsehen, ob das Gerät erfolgreich aktualisiert wurde. Wenn ja, auf „Finish“ (Fertig stellen) klicken, um das Programm zu beenden. Wenn nicht, überprüfen, ob die richtige Datei gewählt wurde, ob das Gerät während der Aktualisierung benutzt wurde und ob das Netzwerk ordnungsgemäß funktioniert. Wenn alles in Ordnung ist und das Gerät trotzdem nicht aktualisiert werden kann, den Xerox-Kundendienst kontaktieren.



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.