

28.09.2006

XEROX-SICHERHEITSMERKBLATT XRX06-004

Kumulatives Update zur Schließung mehrerer Sicherheitslücken

Bei den Versionen 12.050.03.000, 14.050.03.000 und 13.050.03.000 der Systemsoftware für das WorkCentre® bzw. das WorkCentre® Pro handelt es sich um kumulative Updates für die Systemsoftwareversionen 12.027.24.000, 14.027.24.000 und 13.027.24.000 mit Sicherheitskorrekturen. Siehe Anhang A der Patchinstallationsanleitung zur Beschaffung der *.50.03.000-Systemsoftware¹.

Die Aktualisierung auf Systemsoftwareversion 12.050.03.000, 14.050.03.000 bzw. 13.050.03.000 wird dringend empfohlen. Die folgende Tabelle gibt die Version des Netzwerkcontrollers für die jeweilige Systemsoftwareversion an.

Systemsoftwareversion	Netzwerkcontrollerversion
12.050.03.000.	040.010.01172
13.050.03.000.	040.010.51172
14.050.03.000.	040.010.11172

Hintergrundinformation

Versionen 12.050.03.000, 14.050.03.000 und 13.050.03.000 der Systemsoftware stellen Wartungsversionen mit Sicherheitskorrekturen für die Systemsoftwareversionen 12.027.24.000, 14.027.24.000 bzw. 13.027.24.000 dar. Die Aktualisierung enthält Patches für folgende Sicherheitslücken im ESS/Netzwerkcontroller und MicroServer-Webservercode:

- Authentifizierung an der Webbenutzeroberfläche kann umgangen werden
- US-CERT Technical Cyber Security Alert TA04-174A
- Zum Schließen zahlreicher Sicherheitslücken muss Samba-Version aktualisiert werden
- SNMP-Agent meldet keinen Fehler bei schreibgeschützten Objekten
- Fehler-Traps für die SNMP-Authentifizierung können nicht aktiviert bzw. erstellt werden
- Sicherheitslücke des Netzwerkcontrollers: http TRACE XSS attack
- Angefügtes PS-Script führt zum ops3-dmn-Absturz mit Speicherauszug; Dienstverweigerungsangriff (Denial of Service, DoS)
- SMB "Homes" Share sichtbar
- Durchsuchen des Dateisystems über SMB nicht möglich
- Überwachungsprotokoll: anonymer Download möglich
- Probleme mit der HTTP-Sicherheit
- Umgehung der Sicherheitsfunktionen und Start von Alchemy mit USB Thumb Drive (oder anderweitig)
- Funktion "Ablagebereich-SSL-Zertifikat überprüfen" überprüft nicht FQDN
- Bestimmte Dateiberechtigungen sollten eingegrenzt werden
- Linux-Sicherheit: Kernel-Sicherheitslücke CAN-2003-0643 muss geschlossen werden - Socketproblem
- Anschluss 443 ist immer aktiviert - falsche httpd.conf-Konfiguration
- Postgress-Anschlussperre
- Fehler-Traps für die SNMP-Authentifizierung können nicht aktiviert bzw. erstellt werden
- KRITISCHE Fragmente von Restbenutzerdaten in http.log nach sofortigem Überschreiben der Festplatte
- Fehlermeldung am Gerätedisplay beim fehlgeschlagenen sofortigen Überschreiben

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

28.09.2006

- Fehlermeldung durch die Überschreibungsfunktion beim Löschen angehaltener Aufträge
- Überschreibung bei Bedarf schlägt bei Datengrößen über 2 GB fehl

Durch Ausnutzung dieser Sicherheitslücken werden Sicherheitsfunktionen u. U. beeinträchtigt. Angreifer könnten dann Zugriff auf das System erlangen und unerlaubte Änderungen an der Systemkonfiguration vornehmen. Kunden- und Benutzerkennwörter sind jedoch nicht gefährdet.

Betroffene Produkte:

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

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.

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

28.09.2006

wurde. Die Gesetzgebung mancher Länder verbietet den Haftungsausschluss bzw. die Haftungsbeschränkung bei Folgeschäden, so dass die vorgenannten Beschränkungen ggf. nicht zutreffend sind.