

XEROX BEVEILIGINGSBULLETIN XRX05-009

Vanwege zwakke punten in de Xerox MicroServer-webserver is onbevoegde toegang mogelijk.

De volgende softwareoplossing en instructies gelden voor de vermelde producten en zijn bedoeld om uw vertrouwelijke gegevens te beschermen tegen aanvallen via het netwerk.

De softwareoplossing is gecompriemd in een ZIP-bestand van x MB, dat kan worden gedownload via de link in dit bulletin op Xerox.com onder Security:

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

Achtergrondinformatie

De webservercode bevat verschillende zwakke plekken die onbevoegden kunnen aanwenden om zichzelf toegang te verschaffen tot de webserver, waaronder:

- Procedures waarbij verificatie kan worden omzeild.
- Speciaal opgezette HTTP-verzoeken kunnen een denial of service veroorzaken (bijv. een opzettelijke overbelasting van de server zodat toegang onmogelijk wordt) of staan onbevoegden toegang tot bestanden op de aangevallen server toe.
- Cross-site scripting, waardoor de inhoud van websitepagina's door onbevoegden kan worden gewijzigd.

In dat geval zou een aanvaller wijzigingen in de systeemconfiguratie kunnen doorvoeren. Toegangscodes van klanten en/of gebruikers kunnen niet worden achterhaald.

Dit is een cumulatieve patch die tevens de beveiligingspatch omvat die beschreven is in beveiligingsbulletin XRX04-002 (P4) voor de hieronder vermelde producten.

Betreffende producten:

Document Centre®

220

230

332

340

Oplissing

Installatieprocedure WebUI-patch

Bewerkt: 09/08/05

Er is een patch beschikbaar die zwakke plekken in de Xerox MicroServer Web Server verhelpt die zijn gevonden op de multifunctionele eenheden van de Document Centre. De patchsoftware hoeft alleen te worden uitgevoerd als de systeemsoftwareversie van uw multifunctionele apparaat in de onderstaande lijst wordt vermeld. Deze patch vervangt de eerdere patch P4.

De patch is gecomprimeerd in een ZIP-bestand. Download het ZIP-bestand van de vermelde URL en pak het uit op uw bureaublad. De patch dient op de multifunctionele apparaten te worden geïnstalleerd zoals hieronder beschreven. De patch moet naar de apparaten worden gestuurd zoals u deze ontvangen heeft – open niet de bestanden.

Instructies voor de Document Centre 220/230/332/340

Naam patchbestand: **P25_http_DC220-340.dlm**

Vereist voor ESS-versies: **1.12.08 t/m 1.12.85**

Indien uw apparaat over een hogere ESS-versie dan 1.12.87 beschikt, hoeft u de patch niet te installeren.

ESS-softwareversie controleren

Om na te gaan wat de ESS-softwareversie is, kunt u ofwel een configuratieoverzicht afdrukken ofwel de versie opzoeken in de webclientinterface.

Een configuratieoverzicht afdrukken via de lokale gebruikersinterface van het apparaat:

- 1) Druk op de toets Apparaatstatus.
- 2) Selecteer Configuratieoverzicht afdrukken.
- 3) Zoek de informatie over de ESS-softwareversie.

De softwareversie zoeken via de webclientinterface:

- 1) Open een browser en maak verbinding met het multifunctionele apparaat door het IP-adres van het apparaat in te voeren.
- 2) Selecteer het pictogram "Index apparaat" boven in het midden van het scherm.
- 3) Selecteer "**Apparaatprofiel**".
- 4) Blader naar de locatie waar de softwareversie van de ESS wordt weergegeven.

De patch installeren

OPEN HET PATCH-BESTAND NIET, AANGEZIEN U HET DAN MOGELIJK BESCHADIGT.

De patch toepassen via de LPR-methode onder Windows NT, 2000 of XP

Voor deze methode dient het LPD-protocol te zijn ingeschakeld op het apparaat. Controleer in het configuratieoverzicht of het LPD-protocol is ingeschakeld. Dit protocol kan worden ingeschakeld via de lokale gebruikersinterface of via de web-interface. Zie Bijlage A voor instructies.

- 1) Open een DOS-venster met opdrachtregel. U doet dat door in Windows op het pictogram "Start" te klikken en vervolgens "Uitvoeren" te selecteren. Typ "cmd" en druk op <Enter>.
- 2) Verzend het patchbestand via de opdrachtregel: **lpr -S <printer_ip> -P lp P25_http_DC220-340.dlm**
- 3) Zet het apparaat uit en vervolgens weer aan. Wacht tot het apparaat volledig is gestart.
- 4) **Zet nogmaals het apparaat uit en weer aan.**
- 5) De patch is geïnstalleerd wanneer **.P25** is toegevoegd aan het ESS-versienummer.

OPMERKING: Als P25 niet wordt toegevoegd aan het ESS-versienummer, neem dan contact op met het Xerox Welcome Centre om het apparaat te upgraden naar ESS 1.12.85 of de meest recente release.

Bijlage A – Afdrukken via LPD (poort 515) inschakelen

Teneinde de patch te verzenden via de LPR-methode dient uw multifunctionele apparaat Line Printer Daemon (LPD) over poort 515 te ondersteunen. Op de meeste multifunctionele apparaten is deze functie standaard ingeschakeld. Indien LPD-afdrukken is uitgeschakeld, moet u deze functie inschakelen om de LPR-methode te kunnen toepassen.

LPD inschakelen:

- 1) Open een browser en maak verbinding met het multifunctionele apparaat door het IP-adres van het apparaat in te voeren.
- 2) Selecteer het pictogram "Index apparaat" in de rechter bovenhoek.
- 3) Selecteer "Protocollen", blader naar LPD en selecteer de koppeling LPD.
- 4) Indien het selectievakje Ingeschakeld NIET is aangekruist, selecteert u het vakje om een kruisje of vinkje daarin te plaatsen.
- 5) Selecteer "Nieuwe instellingen toepassen".
- 6) Voer de gebruikersnaam en de toegangscode van de beheerder in en selecteer OK.
- 7) Zet het multifunctionele apparaat uit en vervolgens weer aan.

Disclaimer

De informatie in dit productbericht van Xerox wordt zonder enige garantie verstrekt. Xerox Corporation geeft geen enkele garantie, expliciet noch impliciet, inclusief garanties inzake verkoopbaarheid of geschiktheid voor een bepaald doel. In geen geval kan Xerox Corporation aansprakelijk worden gesteld voor enige schade die de gebruiker ondervindt als gevolg van het gebruiken of negeren van de informatie die in dit productbericht van Xerox wordt verstrekt, inclusief directe of indirecte schade, incidentele schade, gevolgschade, winstderving of bijzondere schade, zelfs wanneer Xerox Corporation van tevoren op de mogelijkheid van dergelijke schade is gewezen. Daar waar het uitsluiten of beperken van de aansprakelijkheid voor gevolgschade niet is toegestaan, zal de voorafgaande beperking mogelijk niet van toepassing zijn.