

XEROX BEVEILIGINGSBULLETIN XRX08-001

Er zijn enkele kwetsbare plekken in de ESS/netwerkcontroller die zouden kunnen worden uitgebuit, bijvoorbeeld om ervoor te zorgen dat externe aanvallers willekeurige codes kunnen uitvoeren via speciaal ontworpen RPC-verzoeken (Remote Procedure Call).

De volgende softwareoplossing (patch P32) en toepassingsinstructies worden voor de vermelde producten aangeboden. Deze patch is ontwikkeld voor installatie door de klant. De softwareoplossing wordt tot een zip-bestand van 8,3 MB gecomprimeerd en is te vinden via de volgende koppeling:

http://www.xerox.com/downloads/usa/en/c/cert_P32v2_WCP275_WC7665_Patch.zip

Patch P32 is geclassificeerd als een **belangrijke** patch.

Klanten die zich zorgen maken over deze kwetsbaarheid in de hieronder vermelde producten, moeten aan de hand van de bijgevoegde installatie-instructies eerst controleren of ze een versie hebben, waarop de patch moet worden geïnstalleerd, en, indien dit het geval is, vervolgens de installatie-instructies volgen om de patch te installeren.

- Bij producten uit de WorkCentre®/ WorkCentre® Pro 2xx-serie, systeemsoftwareversie *.60.22.007 of hoger (ESS-controller versie 040.022.x1110 of hoger) is deze oplossing al ingebouwd. Voor deze producten hoeft de patch niet te worden geïnstalleerd.
- Bij WorkCentre® 7655/7665-producten, systeemsoftwareversie 040.032.55080 of hoger (ESS-controller versie 040.032.55080 of hoger) is deze oplossing al ingebouwd. Voor deze producten hoeft de patch niet te worden geïnstalleerd. Bovendien moet voor een WorkCentre® 7655/7665 als de systeemsoftware niet 040.032.53080 of hoger is (Net Controller versie 040.022.*1031 of hoger) een servicemonteur komen om de upgrade van het apparaat naar systeemsoftware/Net Controller versie 040.032.53080 uit te voeren voordat de patch kan worden toegepast.

Opmerking: Deze beveiligingspatch is als patch **P32** geconfigureerd. Wanneer deze patch is geïnstalleerd, geeft de netwerkcontrollerversie **.P32** weer (bijvoorbeeld 040.022.x0115.P32).

Achtergrond

Xerox zet zich voortdurend in om haar klanten te beschermen en heeft de volgende kwetsbare punten gedetecteerd:

- CVE-2007-2446 - Als gevolg van meerdere stapeloverlopen, kunnen er externe codes worden uitgevoerd
- CVE-2007-2447 - Kwetsbaar punt waarop een externe opdracht kan worden ingevoerd

Door deze kwetsbare punten in de ESS/netwerkcontrollercode die het delen van bestanden en printers verwerkt voor SMB-clients (Service Message Block)/CIFS-clients (Common Internet File System), zoals MFD-apparaten van Xerox, kunnen externe aanvallers willekeurige codes uitvoeren, via speciaal hiervoor ontwikkelde RPC-verzoeken (Remote Procedure Call). Deze kwetsbare punten hebben alleen invloed op de deelfuncties van de printer. Als het uitvoeren van de codes lukt, zou een aanvaller wijzigingen in de systeemconfiguratie kunnen doorvoeren. Toegangscodes van klanten en/of gebruikers kunnen niet worden achterhaald.

Deze patch is alleen bedoeld voor op een netwerk aangesloten versies¹ van de volgende producten:

WorkCentre®	WorkCentre Pro®
232	232
238	238
245	245
255	255
265	265
275	275
7655	
7665	

¹Als het product niet op het netwerk is aangesloten, is het niet kwetsbaar en hoeft er geen actie te worden ondernomen.

Oplissing

Installatie-instructies

Patch-bestandsnaam: **WCP275_WC7665_P32v2.dlm**

Deze patch kan op uw systeem worden geïnstalleerd zoals hieronder wordt beschreven.

Overzicht van versies en acties:

- Nagaan wat de systeemsoftwareversie of ESS Controller-versie is
- Nagaan welke upgrades nodig zijn
- Upgrade voor apparaat uitvoeren indien nodig
- Patch toepassen indien nodig

Voor WC/WCP 232/238/245/255/265/275

	Bij de softwareversie systeemsoftware of ESS-controller		Klaar voor patch?	Volgende stap:	Dan:	Netwerkcontroller / ESS toont nu:
1	*.27.24.000 t/m *.27.24.020	040.010.#0930 t/m 040.010.#1160	Nee	Upgrade naar *.60.22.000 of nieuwer. Zie Appendix A	Installeer patch P32	040.022.#1031.BIOSxx.xx.P32v2
2	*.50.03.000 t/m *.50.03.009	040.010.#1172 t/m 040.010.#2250	Nee	Upgrade naar *.60.22.000 of nieuwer. Zie Appendix A	Installeer patch P32	Als de patch wordt toegepast, 040.022.#1031.BIOSxx.xx.P32v2
3	*.50.03.011	040.010.#2280	Nee	Bel Service voor een upgrade naar *.60.22.000 of nieuwer	Installeer patch P32	Als de patch wordt toegepast, 040.022.#1031.BIOSxx.xx.P32v2
4	*.27.24.015 Common Criteria (CC)-certificering	040.010.#1121	Nee	Zie OPMERKING 1 hieronder	-	-
5	*.39.24.001 Common Criteria (CC)-certificering	040.010.#1123	Nee	Zie OPMERKING 1 hieronder	-	-
6	*.60.15.000	040.022.#0112	Nee	Upgrade naar *.60.22.000 of hoger Zie Appendix A	Installeer patch P32	040.022.#1031.BIOSxx.xx.P32v2
7	*.60.17.000 Common Criteria (CC)-certificering	040.022.#0115	Ja	Zie OPMERKING 1 hieronder	-	Als de patch wordt toegepast, 040.022.#0115.P32v2
8	*.60.17.000 t/m *.60.22.006	040.022.#0115 to 040.022.#1100	Ja	Installeer patch P32	-	040.022.#0115.BIOSxx.xx.P32v2 t/m 040.022.#1100.BIOSxx.xx.P32v2
9	*.60.22.0007 en hoger	040.022.#1110 of hoger	NVT	Gereed	-	-

OPMERKING 1: Als uw apparaat systeemsoftwareversie *.27.24.015, *.39.24.001 of *.60.17.000 heeft, dan bevindt uw apparaat zich in de configuratie Common Criteria-certificering. Als u nog niet versie *.60.17.000 heeft, kunt u een upgrade naar *.60.17.000 uitvoeren en vervolgens patch P32 installeren. Het apparaat zal zich echter dan niet langer in de gecertificeerde configuratie Common Criteria bevinden.

Voor WC 7655/7665

	Bij de softwareversie Systeemsoftware of netwerkcontroller		Klaar voor patch?	Volgende stap:	Dan:	Netwerkcontroller / ESS toont nu:
1	040.032.50855 t/m 040.032.51040	040.032.50855 t/m 040.032.51030	Nee	Bel Service voor een upgrade naar 040.032.53080	In- stalleer patch P32	040.032.53080.BIOSxx.xx.P32v2
2	040.032.53080	040.032.53080	Ja	Installeer patch P32	-	040.032.53080.BIOSxx.xx.P32v2
3	Gecertificeerd 040.032.53080 Common Criteria	040.032.53080	Ja	Zie OPMERKING 1 hieronder	-	Als de patch wordt toegepast, 040.032.53080.BIOSxx.xx.P32v2
4	040.032.55030 t/m 040.032.55070	040.032.55030 t/m 040.032.55070	Ja	Zie OPMERKING 1 hieronder	-	Als de patch wordt toegepast, 040.032.55030.BIOSxx.xx.P32v2 t/m 040.032.55070.BIOSxx.xx.P32v2
5	040.032.55080 en hoger	040.032.55080	NVT	Gereed	-	-

OPMERKING 1: Als uw apparaat systeemsoftwareversie 040.032.53080 heeft, dan bevindt uw apparaat zich in de gecertificeerde configuratie Common Criteria. U kunt patch P32 laden. Het apparaat zal zich echter dan niet langer in de configuratie Common Criteria-certificering bevinden.

De patch installeren

U moet de patch downloaden. De patch is gecomprimeerd in een ZIP-bestand. Download het ZIP-bestand van de vermelde URL en pak het uit op een locatie op de vaste schijf of uw bureaublad. Open het bestand met de extensie .DLM niet. Dit is de patch en deze dient als zodanig op het multifunctionele apparaat te worden geïnstalleerd.

Installatiemethoden voor patch

Deze patch en upgrade (zoals de meeste software) kan en moet door de klant worden geïnstalleerd. Er zijn verschillende manieren om dit te doen.

- Zend een Upgrade / Patch-bestand naar het apparaat m.b.v. de webpagina van het apparaat voor de methode Upgrade van de apparaatsoftware.
- Voer een upgrade / of een installatie van een patch uit m.b.v. van een LPR-commando.
- Voer een upgrade / of een installatie van een patch uit voor verscheidene apparaten m.b.v. van LPR-commando's.
- Gebruik XDM en CenterWare Web om Upgrade / Patch-bestanden naar verscheidene apparaten te verzenden.

Raadpleeg voor meer informatie over de bovenstaande methoden de klantentip "How to Upgrade, Patch or Clone Xerox Multifunction Devices" (Het upgraden, patchen of klonen van multifunctionele apparaten van Xerox): (<http://www.office.xerox.com/support/dctips/dc06cc0410.pdf>)

Via een upgrade van de apparaatsoftware

- 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" boven in het midden van het scherm.
- 3) Selecteer "Apparaatsoftware (Upgrades)".
- 4) Voer de gebruikersnaam en de toegangscode in voor het apparaat.
- 5) Selecteer onder "Handmatige upgrade" de toets Bladeren om het bestand **WCP275_WC7665_P32v2.dlm** te zoeken en te selecteren.
- 6) Selecteer de toets "Software installeren".
- 7) Alle WCP's drukken een patchinstallatieblad af en starten automatisch opnieuw om de patch te installeren. De patch is geïnstalleerd wanneer **.P32v2** is toegevoegd aan het versienummer van de netwerkcontroller (ESS).

Appendix A - Systeemsoftware verkrijgen

Zo verkrijgt u systeemsoftwareversies *.60.22.000 of nieuwer:

- a) Gebruik een browser om naar www.xerox.com te navigeren.
- b) Selecteer de koppeling "Support & Drivers".
- c) Selecteer "Multifunction".
- d) Selecteer afhankelijk van uw model "WorkCentre" of "WorkCentre Pro".
- e) Zoek de koppeling voor uw WorkCentre-model.
- f) Selecteer "Drivers & Downloads".
- g) Selecteer de koppeling voor firmware- en apparaatupgrades.
- h) Selecteer de koppeling voor de installatie-instructies van systeemsoftwareset *.60.22.000 en druk deze instructies af of sla ze op.
- i) Selecteer de koppeling voor systeemsoftwareset *.60.22.000" en sla het bestand op uw computer op.
- j) Pak de bestanden op uw bureaublad uit wanneer u deze hebt gedownload.
- k) Lees de opgeslagen installatie-instructies voor de systeemsoftware.
- l) Upgrade het apparaat.

Appendix B – Afdrukken via LPD (poort 515) inschakelen

Teneinde de patch via de LPR-methode te verzenden, 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" of "Index apparaat" in het bovenste deel van het scherm.
- 3) Selecteer "LPR/LPD" of "Line Printer Daemon".
- 4) Indien het selectievakje Ingeschakeld NIET is ingeschakeld, selecteert u het vakje om het in te schakelen.
- 5) Selecteer "Nieuwe instellingen toepassen".
- 6) Voer de gebruikersnaam en de toegangscode van de beheerder in en selecteer OK.
- 7) Start het multifunctionele apparaat opnieuw op via de webpagina Status of door op de aan/uit-toets van het apparaat te drukken.

Disclaimer

De informatie in dit document wordt zonder enige garantie verstrekt. Xerox Corporation geeft geen enkele garantie, noch expliciet noch impliciet, waaronder begrepen, maar niet beperkt tot 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 gebruik van de informatie in dit document, waaronder begrepen, maar niet beperkt tot directe of indirecte schade, gevolgschade, winstderving of bijzondere schade, zelfs wanneer Xerox Corporation van tevoren in kennis is gesteld dat dergelijke schade zich mogelijk zou kunnen voordoen. Daar waar het uitsluiten of beperken van de aansprakelijkheid voor gevolgschade niet is toegestaan, zal de voorafgaande beperking mogelijk niet van toepassing zijn.