FreeFlow Core, Versie 4.0
augustus 2014
708P90734

Xerox® FreeFlow® Core
Beveiligingshandleiding

Documentversie 1.0, augustus 2014

BR10173

Inhoudsopgave

Inhoudsopgave

1

Beveiliging van het pakket FreeFlow-applicaties van Xerox®

Overzicht

Dit document bevat informatie met betrekking tot beveiliging van FreeFlow Core.

Xerox neemt beveiligingskwesties uiterst serieus. Als vooraanstaand bedrijf in de ontwikkeling van digitale technologie verplicht Xerox zich ertoe digitale gegevens te beveiligen door potentiële zwakke plekken op te sporen en proactief aan te pakken om de risico's te beperken. Xerox streeft ernaar het best beveiligde softwareproduct te leveren op basis van de informatie en technologie die op dit moment beschikbaar zijn, en tegelijkertijd de prestaties, waarde, functionaliteit en productiviteit van de producten te handhaven. Er wordt getest of de onderdelen van FreeFlow voldoen aan de beveiligingseisen met behulp van commercieel verkrijgbare scanprogramma's voor de controle van kwetsbaarheid en penetratie. Kwetsbaarheden in de toepassing worden opgelost op basis van de resultaten van onze interne scans.

Firewall inschakelen en configureren

Het wordt aanbevolen om een firewall op de FreeFlow Core-server in te schakelen. Poorten moeten worden geblokkeerd, tenzij ze nodig zijn voor het uitvoeren van een specifieke functie, zoals hieronder uiteengezet:

Poort	Protocol of applicatie	Ingeschakelde FreeFlow Core-functie
80	HTTP	Binnenkomend – De gebruikersinterface van FreeFlow Core starten Uitgaand – Het ophalen van bestanden die in Manifest- of Component-voorinstellingen worden vermeld
161.162	SNMP	Uitgaand – Het identificeren van het DFE-type tijdens de configuratie van de printer
631	IPP	Uitgaand – Het indienen van opdrachten naar DFE's
25, 2525, 465, 475, 587	SMTP	Uitgaand – Het verzenden van e-mailkennisgevingen Opmerking: Benodigde poortnummer is afhankelijk van de configuratie van de SMTP-server
TCP, UDP: 7751	JMF	Binnenkomend – Het ontvangen van JMF/JDF-verzoeken
varieert	JMF	Uitgaand – Het retourneren van JMF-statussignalen. JMF-client specificeert het poortnummer.
139, 445	SMB	Binnenkomend – Het delen van Hot Folders via Windows Bestanden delen Uitgaand – Het gebruik van Hot Folders in gedeelde directory's Uitgaand – Het ophalen van bestanden die in Manifest worden vermeld uit gedeelde directory's Uitgaand – Het ophalen van bestanden die in Components worden vermeld uit gedeelde directory's Uitgaand – Het opslaan naar gedeelde directory's
20,21	FTP	Binnenkomend – Het delen van Hot Folders via FTP Uitgaand - Het ophalen van bestanden die in Manifest- of Component-voorinstellingen worden vermeld
443	HTTPS	Binnenkomend - Het delen van bestanden voor het externe FreeFlow Core-systeem Uitgaand - Het ophalen van bestanden uit het externe FreeFlow Core-systeem

Regels van Windows Firewall

1. Ga naar **Configuratiescherm > Systeem en beveiliging > Windows Firewall > Geavanceerde instellingen**.
2. Selecteer voor elke benodigde regel **Regels voor binnenkomende verbindingen** of **Regels voor uitgaande verbindingen**:
   a) Onder Acties klikt u op **Nieuwe regel**. De Wizard Nieuwe regel voor binnenkomende verbindingen verschijnt.
   b) Klik op **Poort** voor het Regeltype. Klik op **Volgende**.
   c) Klik op **TCP** of **UDP** in overeenstemming met de bovenstaande tabel. Voer een waarde in bij Specifieke lokale poorten in overeenstemming met de bovenstaande tabel. Klik op **Volgende**.
   d) Klik op **De verbinding toestaan.** Klik op **Volgende**.

e) Selecteer alle vakken. Klik op **Volgende**.

Beveiliging tegen virussen

Xerox neemt speciale voorzorgsmaatregelen om er zeker van te zijn dat haar eigen software virusvrij wordt verstuurd. U wordt ten zeerste aangeraden te investeren in virusdetectiesoftware die door de pc-sector wordt geaccepteerd. Ter bescherming van uw systeem tegen virussen is het cruciaal dat uw virusdetectiesoftware up-to-date blijft.

Ter verbetering van de prestaties wordt aanbevolen dat u de installatiedirectory's van FreeFlow Core en de MS SQL-server uitsluit van scans door de antivirussoftware.

U kunt in plaats daarvan ook de volgende FreeFlow Core-mappen uitsluiten van scannen door uw antivirussoftware:

- <FreeFlow Core-installatiedirectory>\Platform\Spool
- <FreeFlow Core-installatiedirectory>\Logs
- <FreeFlow Core-installatiedirectory>\Platform\Logs
- <FreeFlow Core-installatiedirectory>\Web\Logs
- <FreeFlow Core-installatiedirectory>\Config
- <FreeFlow Core-installatiedirectory>\Presets

Software-update

Het wordt aanbevolen dat de klant zorgt dat alle softwareproducten die op de FreeFlow Core-server zijn geïnstalleerd, up-to-date blijven. Microsoft Update moet minimaal een keer per maand worden uitgevoerd.

Service packs voor het besturingssysteem mogen niet worden geïnstalleerd via Microsoft Update totdat ondersteuning via formele communicatie is bevestigd.

Xerox geeft indien nodig maandelijks een veiligheidsbulletin uit met daarin een overzicht van de updates die moeten worden “uitgesloten” op het FreeFlow-systeem. Deze informatie wordt ook bekendgemaakt op de website www.xerox.com/security onder "Product Security Guidance". Updates met een hoge prioriteit en updates die betrekking op de beveiliging hebben, zijn onontbeerlijk en moeten altijd worden geïnstalleerd, tenzij ze specifiek worden uitgesloten.