

Vulnerability affecting FTP print

General Information

Issue Date	2/28/08
Canon Issue ID Number	CVA-001
CVE Identifier Number	CVE-2008-0303
Product Name	imageRUNNER 2230/2830/3530 imageRUNNER 3025/3030/3035/3045 imageRUNNER 2270/2870/3570/4570 imageRUNNER 5070/5570/6570 imageRUNNER 5050/5055/5065/5075 imageRUNNER 8070/85+/9070/105+ imageRUNNER 7086/7095/7105 Color imageRUNNER C3220/2620 Color imageRUNNER C2880/3380 Color imageRUNNER C2550 Color imageRUNNER C4080/4580/5180/5185 Color imageRUNNER LBP5960 Color imageRUNNER LBP5360 imageRUNNER C3170 imageRUNNER C5800/6800 imageRUNNER C5870U/6870U imageRUNNER C5058/5068 imageRUNNER LBP3460 imagePRESS C7000VP imagePRESS C1

Engines listed here using imagePASS, imagePRESS Servers, or ColorPASS devices for printing are NOT affected by this vulnerability.

It was found that certain Canon imageRUNNER, Color imageRUNNER, imagePRESS devices contain a vulnerability known as "FTP bounce" when configured for network printing. Engines using imagePASS, imagePRESS Servers, or ColorPASS devices for printing are NOT affected by this vulnerability.

Overview

In its simplest terms, this vulnerability is based on the potential misuse of the PORT command in the FTP (File Transfer Protocol) in conjunction with command FTP Print.

FTP print is a print method using FTP command. This command is not used for printing from the printer driver. The FTP protocol defines the PORT command, which can be used to establish connections to remote machines other than the FTP client. While this functionality complies with the FTP RFC (Request for Comments – the naming convention used in internet related standards and specifications), it exposes a potential vulnerability known as "FTP bounce", in which a malicious user may, if the FTP print setting is on, be able to utilize the FTP server to open connections which appear to originate from the server.

Impact

In certain devices, a malicious user may exploit this vulnerability to create a connection between the FTP server and other systems on an arbitrary Port. An attacker may be able to scan networks that it would not otherwise have access to. An attacker may also be able to conceal the true origin of a port scanning attempt. However, information in the network host cannot be obtained via the affected machines. Information in the affected machines cannot be obtained or sent, either.

Resolution

To help prevent misuse from occurring, please implement one of the following countermeasures from the device User Interface:

- Customers not using FTP print

1. Navigate to Additional Functions -> System Settings -> Network Settings -> TCP/IP Settings -> FTP print.
2. Set the FTP print to OFF.

- Customers using FTP print

1. Navigate to Additional Functions -> System Settings -> Network Settings -> TCP/IP Settings -> FTP print.
2. Set "user name" and "password" for the FTP print functionality.

If these countermeasures do not meet your security needs, please contact your local Canon Authorized Service Dealer.

Notes

Canon Inc. would like to thank Nate Johnson and the Indiana University for finding and reporting to Canon U.S.A., Inc. this vulnerability.