Xerox Security Bulletin XRX08-007

Software update to address cross site scripting vulnerability

v1.0
06/12/08

Problem

A persistent cross site scripting vulnerability exists in the Web Server of the products listed below. If exploited this vulnerability could allow code injection by malicious web users into the web pages viewed by other users. Customer and user passwords are not exposed.

This vulnerability was reported to us privately by Louhi Networks of Finland. Other than the proof-of-concept exploits code provided by the security researcher, Xerox is not aware of exploit code existing in the field.

Solution

As part of Xerox's on-going efforts to protect customers, executable[1] files containing the network controller software releases addressing this vulnerability are provided for the products listed below. These solutions are designed to be installed by the customer. Please follow the procedures in the "Install Instructions" to install the solutions to protect your product from possible attack through the network.

The software solutions are compressed into one executable file and can be accessed via the URL for each specific product below or via http://www.xerox.com/downloads/usa/en/c/XC110_080519_PS-1.EXE.

- Xerox 4110 Copier/Printer -- http://www.support.xerox.com/go
- Xerox 4590 Copier/Printer -- http://www.support.xerox.com/go
- Xerox 4595 Copier/Printer -- http://www.support.xerox.com/go

Enter the Product Name, and then select Drivers & Downloads under the integrated Copy/Print Server for the specific product.

These solutions are classified as a **Critical** patch.

This software solution applies to network-connected versions[2] of the following products:

- Xerox 4110 Copier/Printer
- Xerox 4590 Copier/Printer
- Xerox 4595 Copier/Printer

[1] Firmware Update Tool for Windows – a firmware upgrade utility bundled with the software release that enables customer installation of the software release

[2] If the product is not connected to the network, it is not vulnerable and therefore no action is required.