HP Analog Fax Accessory 300

Security statement

HP Analog Fax Accessory 300
Security Statement

For HP product models:

LaserJet 4345mfp

LaserJet 9040mfp

LaserJet 9050mfp

Color LaserJet 4730mfp

Color LaserJet 9500mfp

Legal Notice

HP Analog Fax Accessory 300 Security Statement
Rev. 1.06

Contents

Overview.....		1
Fax Firmware.....		1
HP MFP Send Fax driver.....		1
	HP.com and Microsoft Digital Signature.....	1
	Fax PDL.....	2
	PML Objects.....	2
	Hiding Destination Information.....	2
Conclusion.....		2

Overview

The Analog Fax Accessory was designed with one purpose in mind – receiving and sending fax data to and from the MFP it is connected to (LaserJet 4345mfp, 4730mfp, 9040mfp, 9050mfp, 9500mfp). In order to send and receive faxes the product employs a standard fax/data modem card connected to the MFP.

An optional Send Fax driver for a client PC allows the fax job to be initiated remotely from a PC rather than at the MFP control panel. The fax card passes data from the MFP through the public telephone network.

The primary security concerns are gaining network access through the telephone/modem connection and making the MFP or PC vulnerable to a virus or malicious use.

Fax Firmware

Although the Analog Fax Accessory uses a standard modem card, its behavior is strictly controlled by the Analog Fax Accessory firmware using EIA/TIA fax commands and modem control commands (or AT commands). The closed nature of the fax firmware with its limited functionality does not provide a pathway or commands necessary to achieve network access from the telephone network. The only way to create such a path requires a prohibitive engineering effort to build replacement code and install it to the formatter. While there may be other security concerns related to the printer network connection, the Analog Fax Accessory hardware does not add any security risks, as network access is unavailable via the Fax Modem from an external source.

HP MFP Send Fax Driver

The other part of the fax solution is the optional HP MFP Send Fax driver. The Send Fax driver provides an interface to send fax jobs from a PC to an MFP over a network connection. The Send Fax driver software installs on the PC. An MFP firmware update adds support in the MFP for the Send Fax driver.

Hp.com and Microsoft Digital Signature

The driver is available for download from hp.com. The potential security risk involves compromising the driver itself with (for example) a virus or malicious code. However, hp.com is a highly secured website, and Microsoft digitally signs the driver. Modification of the driver would require:

- Intrusion into the hp.com website, and
- A corresponding modification of the digital signing information.

Modifying the driver causes a message to appear during installation, indicating that the driver is not authentic. However, the risk of this occurrence is very low and is no different than downloading and installing other currently available drivers, firmware, or software for the MFP.

Fax PDL

The driver itself running on the client PC provides an additional access point to the MFP through an added Fax PDL (page description language) that is part of the updated MFP firmware. The Fax PDL allows the MFP to accept a fax job sent over the network from the client PC. However, the Fax PDL can only direct received jobs to the fax subsystem, so it is not an entry point to access other parts of the MFP functionality.

Any malicious use of the Fax PDL requires extensive engineering to modify the MFP firmware and install that code into the MFP, but because the Fax PDL specifications are not published, such modifications would be extremely difficult. A simpler assault would be a denial of service (DOS) through the Fax PDL. However, the other PDLs already resident in the MFP are subject to an attack such as this.

- These scenarios require either physical or internal network access to the MFP and thus have a very low risk. In addition, the Fax PDL can be disabled from the control panel if that functionality is not required.

Send Fax jobs received by the MFP are treated the same as walk-up fax jobs for internal information handling (e.g., information temporarily stored on the MFP hard disk). This information is deleted from the disk once the job completes.

- The Send Fax firmware and Fax PDL do not support other activity besides faxing that could expose confidential information which might temporarily reside on the hard disk or in memory.

PML Objects

The Send Fax driver can also retrieve status information from the MFP through some added PML (printer management language) objects. These are read-only objects that provide status on email enable, billing code enable, notification, and Send Fax support installation. These objects are not capable of retrieving other information from the MFP.

Hiding Destination Information

One additional feature to enhance security through the Send Fax driver is the bracket characters ("[" and "]") for use in the destination number. Any numbers enclosed within the brackets do not appear on activity logs and cover sheets. This can be useful if a PIN access code or calling card access number is used in the fax number. The brackets keep this part of the destination number hidden.

Conclusion

In summary, the fax hardware and Send Fax driver software do not increase the likelihood of security intrusions. With the added firmware, Fax PDL, and PML objects to support Send Fax, there are no paths created to allow network access from the phone system. Furthermore, the MFP does not have additional vulnerabilities that could be exploited from inside the network.