Drawer Statement

HP LaserJet Printer Capability Descriptions for North American Electric Reliability Council (NERC) Technical Feasibility Exceptions

Security Level: Public
Date Written: January 26, 2010
Document Source: HP Imaging & Printing Group
HP LaserJet Technical Marketing
Steve.miller3@hp.com

Summary

This document details security capabilities for HP LaserJet printers with respect to North American Electric Reliability Council (NERC) compliance. This information can be used to complete a Technical Feasibility Exception (TFE) for these devices.

The security functionality described applies to all HP LaserJet and HP Color LaserJet printing devices.

CIP-007-R4 - Malicious Software Prevention

HP LaserJet printers use the LynxOS operating system. This is a proprietary Real Time Operating System based on BSD Unix. This Operating System as deployed by HP does not support the use of anti-malware software.

Additionally, LynxOS is not susceptible to Windows based viruses or worms. The ports, protocols and libraries targeted by these vulnerabilities are not present in LynxOS.

CIP-007-R5.3.1, 5.3.2, 5.3.3 - Use of Passwords

The password capabilities supported by these HP LaserJet printers are limited to configuration of the device's web interface, and a 4 character numeric PIN to release stored print jobs. There are no enforcement capabilities for character types, password length, or password expiration.

CIP-007-R6, 6.3 - Security Event Logging

Event Logging in HP LaserJet printers is limited to device and printing errors. It does not provide security event logging for authentication errors, settings changes, or other security related events.