Drawer Statement

HP Color CM8050/CM8060 MFP with Edgeline Technology – Windows XP Embedded Security Concerns

Security Level: Public
Date Written/Updated: April 17, 2007
Document Number: c01119913

Document Summary

- Addresses concerns regarding Microsoft Windows architecture embedded in device.

Introduction

HP CM8050/8060 Color MFPs with Edgeline will be the first HP MFP devices to include a controller running Microsoft Windows technology. This document will address common concerns about Microsoft Windows and their applicability to Edgeline technology.

No Accessibility to the Windows XP Embedded Environment

Edgeline architecture does not allow the user or an attacker to have access to many features that are part of the core operating system. For example, we do not allow users to log in and run programs like they can with a desktop PC. We are able to carefully control exactly what applications and services within Windows XP Embedded are allowed to run. By doing this, we can prevent users from accessing features that have security vulnerabilities.

Edgeline Will Not Require Frequent Microsoft Security Patches

Because Windows desktop operating systems require frequent patches, there is a concern this will apply to Edgeline. The Windows XP Embedded operating system is a modular subset of the full Windows XP operating system. We are able to remove applications and infrastructure that are not needed, reducing exposure to features with vulnerabilities, which reduces our dependence on patches.

By doing this, we estimate that only one or two patches per year will require HP to immediately release a firmware upgrade. Additionally, each time an Edgeline firmware upgrade is released to customers; it will include all Microsoft security hot fixes available at that time.

Edgeline Architecture is Resistant to Windows Viruses

Edgeline's architecture makes it very safe from infection by viruses.

- Incoming email is disabled by default. Even when enabled, email is only processed by the ChaiVM interpreter, so Windows viruses cannot execute.
- Web page processing is not supported. Viruses spread by web pages, such as ActiveX control viruses, cannot run because Edgeline never allows web browsing to arbitrary web pages on the network.
- There are no known document viruses that would affect Edgeline. These viruses are activated when the document is opened by Word or Excel, which cannot happen on the MFP because it is sent only the print-ready version of the document.
- The Host USB connection to Windows XP Embedded is restricted to allow only simple file system and I/O connections. Autorun is disabled, preventing viruses and malware from executing from a USB device.

Edgeline is resistant to attack by worms by default and can be configured to be even more resistant.

- Jetdirect and the LynxOS firmware provide a firewall between the network and the XP Embedded operating system on Edgeline.
- The firewall prevents worms from detecting that Edgeline has Windows XP Embedded installed. Worms that scan the network should ignore Edgeline when they don't detect this Windows "signature".
- Almost all Windows protocols are blocked by the firewall and cannot be accessed by a worm attempting to spread via the network. The few protocols that are allowed through the firewall were analyzed for vulnerabilities and hardened to resist attack.
- The customer can configure Jetdirect to block all network traffic, except from a secure spooler or other known good host PCs. This prevents worms from being able to make any connection to the MFP.

Document Attributes
Product Models: CM8050, CM8060