Topic: **I/Port I8800 Update: Microsoft Security Update MS05-025**
Component(s) Affected: **I/Port I8800, XPe**
Date: **August 23, 2005**

OVERVIEW / ENVIRONMENT

ClearCube has provided a new I/Port update file to improve security on the I8800 I/Port. This update comprises the Microsoft Security Update MS05-025 for Windows XPe as it applies to ClearCube I8800 I/Port devices. MS05-025 is a cumulative update for Internet Explorer that replaces MS05-020, discussed in *Technical Bulletin TB0129*.

Microsoft Security Update MS05-025 is rated by Microsoft as a critical update.

Note: This update applies to the I8800 I/Port only. Do not attempt to install this on other devices.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-025:

http://www.microsoft.com/technet/security/Bulletin/MS05-025.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1211

http://www.kb.cert.org/vuls/id/189754 — A buffer overflow in the Portable Network Graphics (PNG) image rendering component of Microsoft Internet Explorer (IE) may allow a remote attacker to execute code on a vulnerable system. The PNG image format is used as an alternative to other image formats such as the Graphics Interchange Format (GIF). Microsoft Internet Explorer supports the PNG image format. The PNG image rendering component of Microsoft Internet Explorer (`pngfilt.dll`) does not properly handle PNG image files, potentially allowing a buffer overflow to occur. If a remote attacker can persuade a user to access a specially crafted PNG image with IE, that attacker may be able to trigger the buffer overflow.

If a user is logged on with administrative user rights, an attacker who successfully this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0648

An information disclosure vulnerability exists in Internet Explorer because of the way that it handles certain requests to display XML content. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially lead to information disclosure if a user visited this site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could read XML data from another Internet Explorer domain. However, user interaction is required to exploit this vulnerability.

RESOLUTION

To reduce the threat of this vulnerability, install this security update.

This update is provided in a zipped file containing this Technical Bulletin, and these files:

- The local installer, in a folder named **Stand Alone**.
  - A batch file named `Update.bat`
  - A folder named IPORT-CLIENT

ClearCube Technology 8834 Capital of Texas Hwy N Austin, Texas 78759 **voice 512 652 3500** **www.clearcube.com**

- The Grid Center remote installer, in a folder named **GCUpdate**.
  - A batch file named `updateGC.bat`
  - A zipped folder named `IPORT-CLIENT.zip`

The local installer is an executable file that is run by physically carrying the file to the I/Port on a Mass Storage Device such as a key drive, and then executing it.

The Grid Center remote installer is run from the Grid Center Console, in the Update View, and can be applied to multiple I/Ports or I/Port groups simultaneously.

INSTALLING UPDATE LOCALLY

To install an update locally, do the following:

1. Load the update file onto a Mass Storage Device (MSD) such as a key drive.

2. At the I/Port, log in as administrator. Press and hold the Shift key and select **Logoff** from the Start menu. Keep the Shift key depressed until the Administrator Login dialog box is displayed. The factory default Administrator account is `administrator` and the default password is `clearcube`. These can be changed in the User Accounts control panel.

3. Insert the USB storage device into an available USB port.

4. Browse to the folder on the storage device that contains the update file.

5. Double-click the `Update.bat` file. The update installs automatically and reboots the I/Port.

Note: Do not press any keys during the update. Allow it to run undisturbed.

INSTALLING UPDATE REMOTELY USING GRID CENTER

To install an update remotely with Grid Center, do the following:

1. Load the update files onto a volume accessible by the Grid Center Console.

2. Start Grid Center (if it is not already running).

3. From the Update View, select an individual I/Port or an I/Port Group to update.

4. In the I/Port Update View dialog box, enter the path and name of the `IPORT-CLIENT.zip` file (you can browse for this).

5. Enter the path and name of the `updateGC.bat` file (you can browse for this).

6. Press the **Update** button.

7. A dialog box confirming the successful update is displayed when the update is complete. If any I/Ports did not update successfully, a dialog box containing the names of these I/Port is displayed. Write these names down and deploy the update to these I/Ports individually.

8. If an I/Port cannot be successfully updated via Grid Center, attempt to update the I/Port locally (using the first procedure) before contacting ClearCube technical support.

For more information, please contact ClearCube technical support.

support@clearcube.com	Email address for ClearCube Technical Support
support.clearcube.com	ClearCube Support Website
(866) 652-3400	Direct line in the US
+1 (512) 652-3400	Direct line from outside the US