Topic: **I/Port I8800 Update: Microsoft Security Update MS05-014**
Component(s) Affected: **I/Port I8800, XPe**
Date: **March 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 MS05-014 for Windows XPe as it applies to ClearCube I8800 I/Port devices. MS05-014 is a cumulative update for Internet Explorer 6 replaces the MS04-038 update. This update should be installed in combination with MS05-007/-008, described in *Technical Bulletin TB0106JS*.

Microsoft Security Update MS05-014 is rated by Microsoft as a critical update for Windows XP.

Note: ClearCube provided MS04-038 in a combination package with MS04-034, described in *Technical Bulletin TB0102JS*. That combination package should be installed *before* this update, which replaces the MS04-038 update.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-014:

http://www.microsoft.com/technet/security/bulletin/ms05-014.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0053

http://www.kb.cert.org/vuls/id/698835 — Microsoft DHTML Drag-and-Drop events can manipulate Windows to copy objects from one domain to another, including the Local Machine Zone. This vulnerability could allow an attacker to write arbitrary files to the local file system.

See also:

http://www.kb.cert.org/vuls/id/526089 —Microsoft Internet Explorer treats arbitrary files as images for drag and drop operations (MS04-038).

See also:

http://www.kb.cert.org/vuls/id/413886 — Microsoft Internet Explorer allows mouse events to manipulate window objects and perform "drag and drop" operations (MS04-038, "Script in Image Tag File Download Vulnerability").

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0054

http://www.kb.cert.org/vuls/id/580299 — Microsoft Internet Explorer (IE) contains a URL decoding zone spoofing vulnerability that may allow remote attackers to bypass zone security restrictions and execute arbitrary code on affected systems.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0055

http://www.kb.cert.org/vuls/id/843771 — Microsoft Internet Explorer (IE) contains a DHTML method heap memory corruption vulnerability that may allow a remote attacker to execute arbitrary code.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0056

http://www.kb.cert.org/vuls/id/82397 — Microsoft Internet Explorer (IE) contains a Channel Definition Format (CDF) cross-domain vulnerability that may allow unintended information disclosure or remote code execution due to a flaw in handling Channel Definition Format (CDF) files.

ClearCube Technology 8834 Capital of Texas Hwy N Suite 140 Austin, Texas 78759 **voice 512 652 3500** **www.clearcube.com**

RESOLUTION

To reduce the threat of these vulnerabilities, install this security update in combination with MS05-007/-008.

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
- 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:

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