Topic: **I/Port I8800 Update: Microsoft Security Update MS05-038**
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 Microsoft Security Update MS05-038 for Windows XPe as it applies to ClearCube I8800 I/Port devices. This update is a cumulative update for Internet Explorer. MS05-038 replaces MS05-025, discussed in *Technical Bulletin TB1054*, and MS05-037, discussed in *Technical Bulletin TB0156.*

Microsoft Security Update MS05-038 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 MS05-038:

http://www.microsoft.com/technet/Security/bulletin/ms05-038.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1988

http://www.kb.cert.org/vuls/id/965206 — A vulnerability in Internet Explorer's image rendering library that displays JPEG-format files may allow an attacker to craft an image that, when viewed via a web site or an HTML e-mail, could execute arbitrary code on the user's machine. This may create a denial-of-service condition or allow the attacker to take control of the host. This is also known as the JPEG Image Rendering Memory Corruption Vulnerability.

The amount of access an attacker can gain depends on the user's account. If the user is operating with limited privileges, it minimizes the possible impact. However, if the user has administrator privileges, an attacker might be able to gain complete control of the system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1989

A vulnerability in Internet Explorer allows remote attackers to obtain information and possibly execute code when browsing from a web site to a web folder view using WebDAV. This is also known as the Web Folder Behaviors Cross-Domain Vulnerability.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1990

http://www.kb.cert.org/vuls/id/959049

Internet Explorer allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a web page with embedded CLSIDs that reference certain COM objects that are not ActiveX controls which causes memory corruption. This is also known as the COM Object Instantiation Memory Corruption Vulnerability, and is a different vulnerability than CAN-2005-2087, described in **http://www.microsoft.com/technet/Security/bulletin/ms05-037.mspx**, and discussed in *Technical Bulletin TB0156.*

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:

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

- 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:

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