**Topic:** **I/Port I8800 Update: Microsoft Security Update Combination #4**
**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 Microsoft Security Updates MS05-011, MS05-012, MS05-013, and MS05-015 for Windows XPe as they apply to ClearCube I8800 I/Port devices. This update addresses a number of vulnerabilities, as listed in this Technical Bulletin.

Microsoft Security Updates MS05-011, MS05-013, and MS05-015 are rated by Microsoft as critical updates for Windows XP. MS05-012 is rated by Microsoft as an important update for Windows XP.

## DETAILED DESCRIPTION

This vulnerability is addressed in MS05-011:

**http://www.microsoft.com/technet/security/bulletin/ms05-011.mspx**

**http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0045**

**http://www.kb.cert.org/vuls/id/652537** — A vulnerability in the way that Microsoft Windows handles some SMB packets could allow a remote attacker to execute code of their choosing on a vulnerable system.

These vulnerabilities are addressed in MS05-012:

**http://www.microsoft.com/technet/security/bulletin/ms05-012.mspx**

**http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0044**

**http://www.kb.cert.org/vuls/id/927889** — A buffer overflow vulnerability in a way that various programs handle OLE objects could allow a remote attacker to execute arbitrary code on a vulnerable system.

**http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0047**

**http://www.kb.cert.org/vuls/id/597889** — A vulnerability in a way that various programs handle Microsoft COM Structured Storage objects could allow a local attacker to execute arbitrary code on a vulnerable system.

This vulnerability is addressed in MS05-013:

**http://www.microsoft.com/technet/security/bulletin/ms05-013.mspx**

**http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1319**

**http://www.kb.cert.org/vuls/id/356600** — A cross-domain vulnerability exists in the DHTML Editing ActiveX control. An attacker may be able to execute arbitrary script in the Local Machine Zone or read or modify data in other domains. For example, the attacker could execute arbitrary commands with parameters, download and execute arbitrary code, read cookies, spoof content, or modify form behavior.

This vulnerability is addressed in MS05-015:

**http://www.microsoft.com/technet/security/bulletin/ms05-015.mspx**

**http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0057**

**http://www.kb.cert.org/vuls/id/820427** — A buffer overflow exists in the Microsoft Windows system library used when handling hyperlinks. All currently supported versions of Microsoft Windows are affected.



**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. 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:

**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 |