Topic: **I/Port I8800: Microsoft Security Update MS05-052**
Component(s) Affected: **I/Port I8800**
Date: **November 7, 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 MS05-052 for Windows XPe as it applies to ClearCube I8800 I/Port devices. This update is a cumulative update for Internet Explorer. MS05-052 replaces MS05-037, discussed in *Technical Bulletin TB0156*, and MS05-038, discussed in *Technical Bulletin TB0157.*

Microsoft Security Update MS05-052 is rated by Microsoft as a critical update. It is available on the ClearCube Technology Support website as `MS05-052_XPe_CCT.zip`.

For a summary of Microsoft security updates for I8800 I/Ports, please see *Technical Bulletin TB0096JS, Summary of I8800 I/Port Security Updates*. For a summary of other updates for Eon e100 I/Ports, please see *Technical Bulletin TB0161JS, Cumulative List of Updates for I8800 I/Ports*.

Note: This update applies to the I8800 I/Port only. Do not attempt to install this on other devices. For Eon e100 I/Ports, this update is included in the s `E100_XPe_October_2005_Hotfix_Snap-in.zip` file on the ClearCube Technology Support website. See Technical Bulletin *TB0172JS, Eon e100 XPe Update: Microsoft Security Update – October 2005* for more information.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-052:

http://www.microsoft.com/technet/Security/bulletin/ms05-052.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2127 — An attacker who instantiated the Microsoft DDS Library Shape Control (Msdds.dll) and other COM objects in Internet Explorer could take complete control of an affected system. If a user is logged on with administrative user rights, 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 would be less impacted than users who operate with administrative user rights.

http://www.us-cert.gov/cas/techalerts/TA05-284A.html — TA05-284A includes these issues:

- **http://www.kb.cert.org/vuls/id/214572**
- **http://www.kb.cert.org/vuls/id/883460**
- **http://www.kb.cert.org/vuls/id/922708**
- **http://www.kb.cert.org/vuls/id/995220**
- **http://www.kb.cert.org/vuls/id/180868**
- **http://www.kb.cert.org/vuls/id/950516**
- **http://www.kb.cert.org/vuls/id/959049**
- **http://www.kb.cert.org/vuls/id/680526**

VU#214572 — Microsoft Plug and Play fails to properly validate user supplied data in the handling of message buffers. This may result in local or remote arbitrary code execution or denial-of-service conditions. (CAN-2005-2120)

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

VU#883460 — A buffer overflow in Microsoft Collaboration Data Objects may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system. (CAN-2005-1987)

VU#922708 — Microsoft Windows Shell fails to handle shortcut files properly
Microsoft Windows Shell does not properly handle some shortcut files and may permit arbitrary code execution when a specially-crafted file is opened. (CAN-2005-2122)

VU#995220 — A buffer overflow in Microsoft DirectShow may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable system. (CAN-2005-2128)

VU#180868 — The Microsoft Distributed Transaction Coordinator (MSDTC) may be vulnerable to a buffer overflow via a specially crafted network message that allows remote, unauthenticated attackers to execute arbitrary code. (CAN-2005-2119)

VU#950516 — Microsoft COM+ contains a vulnerability due to a memory management flaw that may allow an attacker to take complete control of an affected system. (CAN-2005-1978)

VU#959049 — Microsoft Internet Explorer may initialize COM objects that were not intended to be used in the web browser, causing memory corruption. Several COM objects have been identified that may allow an attacker to execute arbitrary code or crash Internet Explorer. (CAN-2005-1990, CAN-2005-2127)

VU#680526 - Microsoft Internet Explorer allows non-ActiveX COM objects to be instantiated
Microsoft Internet Explorer may allow non-ActiveX COM objects to be instantiated that were not intended to be used in the web browser . This may allow an attacker to execute arbitrary code or crash Internet Explorer. (CAN-2005-0163)

RESOLUTION

To reduce the threat of these vulnerabilities, install this security update.

This update is provided in a zipped file is available on the ClearCube Technology Support website as `MS05-052_XPe_CCT.zip` 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