Topic: I/Port I8800 Update: Microsoft Security Update Combination #3
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 MS05-007 and MS05-008 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.

This update should be installed in combination with MS05-014, described in *Technical Bulletin TB0108JS*.

Microsoft Security Update MS05-007 is rated by Microsoft as a moderate update for Windows XP. MS05-008 is rated by Microsoft as an important update for Windows XP.

DETAILED DESCRIPTION

This vulnerability is addressed in MS05-007:

http://www.microsoft.com/technet/security/bulletin/ms05-007.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0051

http://www.kb.cert.org/vuls/id/939074 — The Microsoft Windows XP named pipe fails to restrict anonymous access, and can leak authentication information.

This vulnerability is addressed in MS05-008:

http://www.microsoft.com/technet/security/bulletin/ms05-008.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 are insufficiently validated, and 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.

Microsoft Drag-and-Drop events do not properly validate objects before placing them on a user's system. For more information concerning Drag-and-Drop vulnerabilities, refer to:
http://www.kb.cert.org/vuls/id/526089 — Microsoft Internet Explorer (IE) treats arbitrary files as images for drag and drop operations. This could allow an attacker to trick a user into copying a file to a location where it may be executed, such as the Windows StartUp folder. (0102, 0108)
and
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"). (0102, 0108)

According to Microsoft:

> *"The update for the "Drag-and-Drop Vulnerability" (CAN-2005-0053) comes in two parts. It is addressed in part in this security bulletin. This security bulletin [MS05-008], together with security bulletin MS05-014, makes up the update for CAN-2005-0053. These updates do not have to be installed in any particular order. However, we recommend that you install both updates." (Source: Microsoft)*

MS05-014 creates and installs a list of file types within Internet Explorer that are allowed to be transferred via a Drag-and-Drop event. MS05-008 introduces a more strict validation procedure for Drag-and-Drop events within the Windows shell. For more information on these vulnerabilities and their remediation, please see MS05-014 and MS05-008, as well as MS04-038. *(Source: US-CERT)*

TB0106 rev 8/24/2005

RESOLUTION

To reduce the threat of these vulnerabilities, install this security update, in combination with MS05-014.

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