Topic: **I/Port I8800 Update: Microsoft Security Update Combination #7**
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 Updates MS05-036 and MS05-037 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 MS05-036 and MS05-037 are rated by Microsoft as critical updates.

Note: This update applies to the I8800 I/Port only. Do not attempt to install this on other devices.

DETAILED DESCRIPTION

This vulnerability is addressed in MS05-036:

http://www.microsoft.com/technet/security/Bulletin/MS05-036.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1219

A remote code execution vulnerability in the way that the Microsoft Color Management Module handles ICC profile format tag validation could allow an attacker who successfully exploited this vulnerable to take complete control of an affected system. If a user is logged on with administrative user rights, an attacker could take complete control of an affected system. 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 could be less impacted than users who operate with administrative user rights.

This vulnerability is addressed in MS05-037:

http://www.microsoft.com/technet/security/Bulletin/MS05-037.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2087

http://www.kb.cert.org/vuls/id/939605 — A vulnerability exists in the JView Profiler (`Javaprxy.dll`) that may allow an attacker to take complete control of the affected system. If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. 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 could be less impacted than users who operate with administrative user rights.

The JView Profiler is a COM object provided by `javaprxy.dll`, which is an interface to the debugger in the Microsoft Java Virtual Machine. Internet Explorer attempts to instantiate any COM object that is referenced by a web page. COM objects that are not ActiveX controls may cause unexpected results, such as crashing Internet Explorer. The JView Profiler COM object crashes in a way that can be exploited to execute arbitrary code on a vulnerable system.

By convincing a user to view a specially crafted HTML document (e.g., a web page or an HTML email message), an attacker could execute arbitrary code with the privileges of the user. The attacker could also cause IE (or the program using the WebBrowser control) to crash.

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

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:

- 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