Topic:	**I/Port I8800 Update: Microsoft Security Update Combination #6**
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 MS05-026, MS05-027, and MS05-028 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. MS05-026 replaces MS03-044, MS04-023, and MS05-001, discussed in *Technical Bulletin TB0105JS*. MS05-027 replaces MS032-070 and MS03-024.

Microsoft Security Updates MS05-026 and MS05-027 are rated by Microsoft as critical updates. Microsoft Security Update MS05-028 is rated by Microsoft as an important update. This update package should be considered a critical update.

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 MS05-026:

http://www.microsoft.com/technet/security/Bulletin/MS05-026.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1208

http://www.kb.cert.org/vuls/id/851869 — An integer overflow vulnerability exists in the Microsoft HTML Help system that could allow remote code execution on an affected system. HTML Help is the standard help system for the Windows platform. HTML Help components can be compiled to compress HTML, graphic, and other files into a relatively small `.chm` compiled help file. The resulting `.chm` file can then be distributed with a software application or downloaded from the Web. The Help Viewer application uses the underlying components of Microsoft Internet Explorer to display help content.

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 are less impacted than users who operate with administrative user rights.

This vulnerability is addressed in MS05-027:

http://www.microsoft.com/technet/security/Bulletin/MS05-027.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1206

http://www.kb.cert.org/vuls/id/489397 — A buffer overflow vulnerability in Server Message Block (SMB) could allow an attacker to take complete control of the affected system. Server Message Block is a protocol which allows sharing of files, printers, serial ports, and other abstractions. The SMB protocol is supported on many platforms and architectures. The Microsoft Server Message Block implementation contains a flaw in incoming SMB packet validation that may result in a buffer receiving inappropriate data. An attacker may send a specially-crafted SMB packet to the vulnerable host and be able to execute arbitrary code on the host after exploiting the incoming packet processing flaw. The attacker-supplied code would be run in the context of Local System, resulting in a complete compromise of the system.

This vulnerability is addressed in MS05-028:

http://www.microsoft.com/technet/security/Bulletin/MS05-028.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1207

A buffer overflow in the Web Client service in Microsoft Windows XP allows remote authenticated users to execute arbitrary code via a crafted WebDAV request containing special parameters. 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.

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