Topic: **I/Port I8800 Update: Microsoft Security Update Combination #9**
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 the following Microsoft Security Updates:

- MS05-044
- MS05-045
- MS05-047
- MS05-050

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 Update MS05-050 is rated by Microsoft as a critical update, and replaces MS03-030. Microsoft Security Update MS05-047 is rated by Microsoft as an important update. MS05-047 replaces MS05-039, discussed in *Technical Bulletin TB0158JS*. Microsoft Security Updates MS05-044 and MS05-045 are rated by Microsoft as moderate updates for Windows XP.

This update package should be considered a critical update. It is available on the ClearCube Technology Support website as `MS05-044_045_047_050_combo_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 `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

This vulnerability is addressed in MS05-044:

http://www.microsoft.com/technet/Security/bulletin/ms05-044.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2126

http://www.kb.cert.org/vuls/id/415828 — A vulnerability in the way the Windows FTP client validates file names could allow an attacker to write files to arbitrary locations. If the target location is the Startup folder, then it is possible to cause arbitrary code to be automatically executed the next time the user logs in. User interaction is required before the file can be transferred to the affected system. Exploit code for this vulnerability is publicly available.

This vulnerability is addressed in MS05-045:

http://www.microsoft.com/technet/Security/bulletin/ms05-045.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2307 — A denial of service vulnerability exists in the Network Connection Manager. An attacker who successfully exploited this vulnerability

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

could cause the component responsible for managing network and remote access connections to stop responding. If the affected component is stopped due to an attack, it automatically restarts when new requests are received.

An attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited by anonymous users. However, remote authenticated users could attempt to exploit this vulnerability. In certain configurations, anonymous users could authenticate as the Guest account.

This vulnerability is addressed in MS05-047:

http://www.microsoft.com/technet/Security/bulletin/ms05-047.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2120

http://www.kb.cert.org/vuls/id/214572 — A remote code execution vulnerability exists in Plug and Play (PnP) that could allow an authenticated attacker to take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker must have valid logon credentials to try to exploit this vulnerability. The vulnerability could not be exploited remotely by anonymous users. However, the affected component is available remotely to users who have standard user accounts.

This vulnerability is similar to the issue reported in MS05-039 **http://www.kb.cert.org/vuls/id/998653**. However, the issue reported in MS05-047 **http://www.kb.cert.org/vuls/id/214572** is only exploitable by remote, authenticated attackers on Windows XP SP1. This security update replaces MS05-039.

Proof-of-concept exploit code has been made public, with the implication that this is being routinely exploited.

This vulnerability is addressed in MS05-050:

http://www.microsoft.com/technet/Security/bulletin/ms05-050.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2128

http://www.kb.cert.org/vuls/id/995220 — A remote code execution vulnerability exists in DirectShow (part of Windows Media Player 9) that could allow an attacker who successfully exploited this vulnerability to gain the same user rights as the local user. 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 security update replaces MS03-030.

Note: DirectX is not installed in the I8800 factory system image.

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 `MS05-045_047_048_050_combo_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