Topic:	**I/Port I8800 Update: Microsoft Security Combination #1**
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 MS04-034 and MS04-038 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. MS04-034 replaces MS02-054, a previous update; MS04-038 replaces MS04-025 and represents a cumulative update for Microsoft Internet Explorer.

Microsoft Security Updates MS04-034 and MS04-038 are rated by Microsoft as critical updates for Windows XP.

DETAILED DESCRIPTION

This vulnerability is addressed in MS04-034:

http://www.microsoft.com/technet/security/bulletin/ms04-034.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0575

http://www.kb.cert.org/vuls/id/649374 — A buffer overflow exists in the way Microsoft Windows processes zip files that may allow remote code execution. Microsoft Windows XP features the ability to natively handle .zip files. Microsoft has released bulletin MS04-034 describing a remotely exploitable buffer overflow vulnerability in the way Windows handles zip files. According to MS04-034:

> *"A remote code execution vulnerability exists in Compressed (zipped) Folders because of an unchecked buffer in the way that it handles specially crafted compressed files. An attacker could exploit the vulnerability by constructing a malicious compressed file that could potentially allow remote code execution if a user visited a malicious Web site. An attacker who successfully exploited this vulnerability could take complete control of an affected system. However, user interaction is required to exploit this vulnerability." (source: Microsoft)*

These vulnerabilities are addressed in MS04-038:

http://www.microsoft.com/technet/security/bulletin/ms04-038.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0216

http://www.kb.cert.org/vuls/id/637760 — The Active Setup Install Engine in Microsoft Internet Explorer contains a buffer overflow vulnerability that may allow an attacker to take complete control of a vulnerable system. The Active Setup Install Engine (`inseng.dll`) permits cabinet files to be launched and executed. Cabinet files are archives used to store the various files used by ActiveX controls. The Install Engine, which decompresses these cab files, contains a buffer overflow vulnerability. An attacker could exploit this vulnerability by convincing a user to install an ActiveX control that is contained in a specially crafted cabinet file.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0727

http://www.kb.cert.org/vuls/id/207264 — Microsoft Internet Explorer (IE) fails to properly validate function redirection. The impact is similar to that of a cross-site scripting vulnerability, which allows an attacker to access data in other sites, including the Local Machine Zone.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0839

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.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0841

http://www.kb.cert.org/vuls/id/413886 — Microsoft Internet Explorer (IE) allows dynamic HTML (DHTML) mouse events to manipulate window objects and perform "drag and drop" operations 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.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0842

http://www.kb.cert.org/vuls/id/291304 — Microsoft Internet Explorer (IE) contains a buffer overflow vulnerability in the way that IE processes Cascading Style Sheets (CSS). This may allow an attacker to execute arbitrary code or cause a denial of service. An attacker can exploit this vulnerability by creating a specially crafted style sheet that causes a buffer overflow and heap memory corruption. The buffer overflow can be triggered by viewing an HTML document such as a web page or email message.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0843

http://www.kb.cert.org/vuls/id/625616 — Microsoft Internet Explorer (IE) contains a vulnerability in its handling of navigation commands from plug-ins. This could let an attacker spoof the address of a website. IE improperly handles navigations from plug-ins, such as ActiveX controls. This improper navigation handling could cause IE to display an incorrect URL in the Address bar. As a result, a web site operator could make it appear that the content from his or her web site actually originated from another site when, in fact, it did not.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0844

http://www.kb.cert.org/vuls/id/VU#431576 — Microsoft Internet Explorer (IE) contains a vulnerability in how it processes URLs on Double Byte Character Set (DBCS) systems. This could allow an attacker to spoof the address of a web site.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0845

http://www.kb.cert.org/vuls/id/795720 — Microsoft Internet Explorer (IE) fails to properly validate cached HTTPS contents, allowing an attacker to obtain information or spoof information on a secure web site. The HTTPS protocol is used to provide authentication, encryption, integrity, and non-repudiation services to web applications. IE does not properly validate cached HTTPS content. An attacker could exploit this vulnerability by creating a web site with the same host name as the legitimate HTTPS protected web site. When the attacker's web site is viewed, the contents are cached. If the attacker redirects the victim's browser to the legitimate web site, the attacker's cached contents are then displayed within the context of that web site. The cached content could include script code, images, or other locally cached items.

RESOLUTION

To reduce the threat of these vulnerabilities, 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