Topic: **I/Port I8800 Update: Microsoft Security Update MS05-020**
Component(s) Affected: **I/Port I8800, XPe**
Date: **April 26, 2005**

OVERVIEW / ENVIRONMENT

ClearCube has provided a new I/Port update file to improve security on the I8800 I/Port. This update comprises the Microsoft Security Update MS05-020 for Windows XPe as it applies to ClearCube I8800 I/Port devices. This update addresses a number of remote code execution vulnerabilities, as listed in this Technical Bulletin. This update replaces a previous Microsoft update, MS05-014, discussed in *Technical Bulletin TB0108JS*.

Microsoft Security Update MS05-020 is rated by Microsoft as a critical update for Windows XP.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-020:

http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0553

http://www.kb.cert.org/vuls/id/774338 — Microsoft Internet Explorer contains a vulnerability in the way that it handles DHTML Objects. Dynamic HTML (DHTML) is built on an object model that extends the traditional static HTML document, which enables Web authors to create more engaging and interactive Web pages.

By convincing a user to view a malformed DHTML document (e.g., a web page or HTML email message), an attacker could execute arbitrary commands or code with the privileges of the user. If a user is logged on with administrative user rights, an attacker who successfully exploited any of these vulnerabilities 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.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0554

http://www.kb.cert.org/vuls/id/756122 — Microsoft Internet Explorer (IE) contains a remote code execution vulnerability because of the way that it handles certain URLs. The process that checks the URL contains a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code on a vulnerable system.

By convincing a user to view an HTML document (e.g., a web page or HTML email message), an attacker could execute arbitrary commands or code with the privileges of the user. The attacker could take any action as the user. If the user has administrative privileges, the attacker could take complete control of the user's system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0555

http://www.kb.cert.org/vuls/id/222050 — A buffer overflow in Microsoft Internet Explorer Content Advisor may allow a remote attacker to execute arbitrary code on a vulnerable system. The Content Advisor is used to control what content is viewable in Internet Explorer. A buffer overflow exists in the routines that handle Content Advisor files. If an attacker can persuade a user to visit a specially crafted web page, the attacker may be able to execute arbitrary code with the privileges of the current user. If the user has administrative privileges, the attacker could take complete control of the user's system. A user would need to click through a series of Content Advisor setup windows for the attack to be successful.

For each of these vulnerabilities, CERT recommends that, in addition to installing a security update, do the following:

- Do not install unsolicited Content Advisor files.

  This vulnerability could be exploited when a user installs a Content Advisor (.rat) file. Do not open files of this type.

- Disable Active scripting and ActiveX controls.

  To protect against this and other IE vulnerabilities, consider disabling Active scripting and ActiveX controls in the Internet Zone as described in the Malicious Web Scripts FAQ. Consider disabling Active scripting and ActiveX controls in the Local Machine Zone. See *Microsoft Knowledge Base Article 833633* for information about securing the Local Machine Zone and *Microsoft Knowledge Base Article 315933* for information about displaying the Local Machine Zone (My Computer security zone) on the Security tab in the Internet Options dialog box.

  Note that disabling Active scripting and ActiveX controls in the Internet Zone will reduce the functionality of some web sites. Disabling these features in the Local Machine Zone will reduce the functionality of some programs, including the Help and Support Center in Windows XP.

- Read and send email in plain text format.

  Outlook 2003, Outlook 2002 SP1, and Outlook 6 SP1 can be configured to view email messages in text format. Consider the security of fellow Internet users and send email in plain text format when possible. Note that reading and sending email in plain text will not necessarily prevent exploitation of this vulnerability.

- Do not follow unsolicited links.

  In order to convince users to visit their sites, attackers often use URL encoding, IP address variations, long URLs, intentional misspellings, and other techniques to create misleading links. Do not click on unsolicited links received in email, instant messages, web forums, or internet relay chat (IRC) channels. Type URLs directly into the browser to avoid these misleading links. While these are generally good security practices, following these behaviors will not prevent exploitation of this vulnerability in all cases, particularly if a trusted site has been compromised or allows cross-site scripting.

RESOLUTION

To reduce the threat of this vulnerability, install this security update. Consider also CERT's recommendations on general internet security, described in the previous section.

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.

To 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