Topic: **I/Port I8800 Update: Microsoft Security Update Combination #8**
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 the following Microsoft Security Updates:

- MS05-039
- MS05-040
- MS05-041
- MS05-042
- MS05-043

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 MS05-039 and MS05-043 are rated by Microsoft as critical updates for Windows XP. Microsoft Security Update MS05-040 is rated by Microsoft as an important update. Microsoft Security Updates MS05-041 and MS05-042 are rated by Microsoft as moderate updates. 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 MS05-039:

http://www.microsoft.com/technet/Security/bulletin/ms05-039.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1983

http://www.kb.cert.org/vuls/id/998653 — A stack-based buffer overflow in the Plug and Play (PnP) service for Microsoft Windows 2000 and Windows XP Service Pack 1 allows remote attackers to execute arbitrary code via a specially crafted packet, and local users to gain privileges via a malicious application, as exploited by the Zotob (aka Mytob) worm. While this vulnerability applies primarily to Windows 2000, a previously compromised Windows XP system could be affected as well.

This vulnerability is addressed in MS05-040:

http://www.microsoft.com/technet/Security/bulletin/ms05-040.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0058 — A remote code execution vulnerability exists in the Telephony Application Programming Interface (TAPI) that could allow an attacker to elevate privileges or execute arbitrary code. An attacker who successfully exploited this vulnerability could take complete control of an affected system and then install programs; view, change, or delete data; or create new accounts with full user rights.

This vulnerability is addressed in MS05-041:

http://www.microsoft.com/technet/Security/bulletin/ms05-041.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1218

http://www.kb.cert.org/vuls/id/490628 — An input validation error in the Microsoft Remote Desktop Protocol (RDP) service may allow a remote attacker to send a specially crafted RDP message and cause a denial-of-service condition by causing the system to stop responding. The RDP service is not enabled by default on Microsoft Windows, but the Microsoft Firewall allows RDP traffic to enter a system on TCP port 3389 by default. The I/Port communication model relies on both RDP and TCP port 3389. Exploit code for this vulnerability is publicly available.

These vulnerabilities are addressed in MS05-042:

http://www.microsoft.com/technet/Security/bulletin/ms05-042.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1981 — A denial of service vulnerability exists that could allow an attacker to send a specially crafted message to a Windows domain controller that could cause the user authentication service in an Active Directory domain to stop responding. An attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited by anonymous users.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1982 — An information disclosure and spoofing vulnerability could allow a local user to obtain information and spoof a server via a man-in-the-middle (MITM) attack between a client and a domain controller. Users could believe they are accessing a trusted server when in reality they are accessing a malicious server. However, an attacker would first have to inject themselves into the middle of an authentication session between a client and a domain controller. An attacker must have valid logon credentials and be able inject themselves into the middle of an authentication session between a client and a domain controller to exploit this vulnerability. The vulnerability could not be exploited by an anonymous user.

This vulnerability is addressed in MS05-043:

http://www.microsoft.com/technet/Security/bulletin/ms05-043.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1984

http://www.kb.cert.org/vuls/id/220821 — A remote code execution vulnerability exists in the Printer Spooler service that could allow an attacker to take complete control of the affected system. The Print Spooler service (`sploolsv.exe`) does not properly handle incoming messages, potentially allowing a buffer overflow to occur. If a remote attacker can convince a user to connect to a malicious print server, that attacker may be able to trigger the buffer overflow. An unauthenticated remote attacker may be able to execute arbitrary code on a vulnerable system. In addition, this vulnerability can be exploited locally by an attacker that has a valid user account on a vulnerable system.

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