Topic: **I/Port I8800 Update: Microsoft Security Update Combination #5**
Component(s) Affected: **I/Port I8800, XPe**
Date: **August 24, 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 MS05-018 and MS05-019 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.

MS05-018 replaces MS03-045 and MS05-002, discussed in *Technical Bulletin TB0105JS*. Microsoft Security Update MS05-018 is rated by Microsoft as an important update for Windows XP SP1.

Microsoft Security Update MS05-019 is rated by Microsoft as a critical update for Windows XP SP1.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-018:

http://www.microsoft.com/technet/security/bulletin/ms05-018.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0060

http://www.kb.cert.org/vuls/id/ 943749 — A buffer overflow in the font processing component of Windows XP could allow a locally authenticated user to take complete control of an affected system. Microsoft indicates that this vulnerability could not be exploited remotely.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0061

http://www.kb.cert.org/vuls/id/775933 — A privilege elevation vulnerability exists in the way that the Windows' kernel processes certain access requests. This vulnerability could allow a logged-on user to take complete control of the system. Microsoft indicates that this vulnerability could not be exploited remotely.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0550

http://www.kb.cert.org/vuls/id/650181 — A buffer overflow vulnerability in Microsoft Object Management code exists that could be attacked by sending specially crafted requests locally on an affected operating system. An attacker who exploited this vulnerability could cause the affected system to stop responding and automatically restart. Repeated exploitation of this vulnerability may result in a sustained denial of service. Microsoft indicates that this vulnerability could not be exploited remotely; an attacker would have to be a locally authenticated user.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0551

http://www.kb.cert.org/vuls/id/259197 — A stack-based buffer overflow in `WINSRV.DLL` in the Client Server Runtime System (CSRSS) incorrectly validates certain messages, potentially resulting in privilege elevation. CSRSS is the user-mode part of the Win32 subsystem, which must be running at all times. CSRSS is responsible for console windows, for creating and deleting threads, and for some parts of the 16-bit virtual MS-DOS environment. The CSRSS responds only to requests made by other processes on the local computer. A locally authenticated user may be able to exploit a vulnerability in the way CSRSS validates certain messages in order to gain elevated privileges and complete control of the system.

These vulnerabilities are addressed in MS05-019:

http://www.microsoft.com/technet/security/bulletin/ms05-019.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0048

http://www.kb.cert.org/vuls/id/233754 — Microsoft Windows does not adequately validate IP options, allowing an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service. Since the IP stack is implemented as a kernel driver, an attacker who successfully executes arbitrary code could gain complete control of a vulnerable system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0790

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-1060

http://www.kb.cert.org/vuls/id/222750 — TCP/IP implementations do not adequately validate ICMP error messages. A remote attacker could cause TCP connections to drop or be degraded using spoofed ICMP error messages. Applications that depend on long-lived, low latency, or high throughput TCP connections may not function correctly on a degraded TCP connection. In order to spoof an ICMP message, an attacker would need to know or guess the source and destination TCP port and IP address.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0230

http://www.us-cert.gov/cas/bulletins/SB05-068.html — A vulnerability exists that affects implementations of the Transmission Control Protocol (TCP) that comply with the Internet Engineering Task Force's (IETF's) Requests For Comments (RFCs) for TCP. The impact of this vulnerability varies by vendor and application, but could let a remote malicious user cause a Denial of Service, or allow unauthorized malicious users to inject malicious data into TCP streams.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-0688

http://www.kb.cert.org/vuls/id396645 — Some versions of Windows are vulnerable to a denial-of-service attack via a crafted TCP packet. The packet is spoofed in a manner such that the source and destination IP addresses are the same, the source and destination ports are the same, and the SYN flag is set. Upon receiving such a packet, Windows may become unresponsive for several seconds. This type of attack is known as a LAND attack.

By sending a specially crafted TCP packet to a Windows machine, an attacker could cause excessive CPU usage on the target system. Repeated exploitation of this vulnerability could result in a sustained denial-of-service condition.

Network firewall, Intrusion Detection and Prevention Systems, and packet filtering technology may be able to detect and block LAND attacks. If a perimeter network device is configured to drop incoming packets with source IP addresses that match addresses within the network, a remote attacker may not be able to exploit this vulnerability.

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.

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