Topic: **I/Port I8800 Update: Microsoft Security Update MS04-011**
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 the Microsoft Security Update MS04-011 for Windows XPe as it applies to ClearCube I8800 I/Port devices. Microsoft Security Update MS04-011 addresses a number of vulnerabilities as described in this Technical Bulletin. Related vulnerabilities are described in MS04-028 (*Technical Bulletin TB0100JS*) and MS04-032 (*Technical Bulletin TB0101JS*). The updates provided with these three Security Updates should all be installed to provide the maximum protection. This update replaces MS04-007.

One of the vulnerabilities addressed by MS04-011 is a buffer overrun vulnerability in the Local Security Authority Subsystem Service (LSASS). The Sasser virus exploits weaknesses in LSASS. ClearCube has previously released an I/Port I8800 update to remove the Sasser virus. See *Technical Bulletin TB0093MH, I8800 I/Port Update: Sasser Virus Scanner*.

Note: A similar update is available for the Sasser virus, an Internet worm spread through a buffer overrun vulnerability in the Local Security Authority Subsystem Service (LSASS) vulnerability, as documented in Microsoft Security Bulletin **MS04-011**. See *Technical Bulletin TB0093MH, I8800 I/Port Update: Sasser Virus Scanner*.

Microsoft Security Update MS04-011 is rated by Microsoft as a critical update for Windows XP.

DETAILED DESCRIPTION

These vulnerabilities are addressed in MS04-011:

http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533

http://www.kb.cert.org/vuls/id/753212 — The Windows Local Security Authority Service Server (LSASS) contains a buffer overflow in the `DsRolepInitializeLog()` function that may permit an attacker to completely compromise the system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719

http://www.kb.cert.org/vuls/id/586540 — A vulnerability exists in the Microsoft Private Communications Transport (PCT) protocol, which is part of the Microsoft Secure Sockets Layer (SSL) library, that fails to properly validate message inputs. Exploitation of this vulnerability may permit a remote attacker to compromise the system. An exploit for this issue is currently being used to compromise vulnerable systems running SSL-enabled IIS 5.0. This vulnerability exists in any SSL-enabled program running on vulnerable Windows systems. Windows 2003 Server is not affected if PCT is disabled.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0806

http://www.kb.cert.org/vuls/id/471260 — The Microsoft Windows Logon process (Winlogon) contains a buffer overflow vulnerability that may permit a remote attacker to execute arbitrary code on the system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0906

http://www.kb.cert.org/vuls/id/547028 — A buffer overflow vulnerability exists in the APIs that handle Microsoft Windows Metafiles (WMF) and Enhanced Metafiles (EMF) image formats. Exploitation may lead to an attacker executing arbitrary code on the system.

ClearCube Technology 8834 Capital of Texas Hwy N Suite 140 Austin, Texas 78759 **voice 512 652 3500** **www.clearcube.com**

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0907

http://www.kb.cert.org/vuls/id/260588 — A remotely exploitable vulnerability exists in the Microsoft Windows Help and Support Center (HCP). An attacker could compromise the victim's system by tricking them into visiting a malicious web site, or viewing a malicious email message.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0909

http://www.kb.cert.org/vuls/id/n206468 — Microsoft Windows XP contains a vulnerability in the way that tasks are created that may permit an authenticated user to launch applications with elevated privileges.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0117

http://www.kb.cert.org/vuls/id/353956 — A vulnerability in Microsoft Windows' implementation of the multimedia telephony protocol H.323 could lead to the ability to remotely execute arbitrary code on the system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0119

http://www.kb.cert.org/vuls/id/n638548 — The Microsoft Windows Security Software Provider (SSP) interface fails to properly validate values used during authentication protocol selection. This remotely exploitable vulnerability could permit an attacker to execute arbitrary code on the system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0120

http://www.kb.cert.org/vuls/id/150236 — A vulnerability in the Microsoft Secure Sockets Layer (SSL) library could allow a remote attacker to cause a denial-of-service (DoS) condition on an affected system.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0123

http://www.kb.cert.org/vuls/id/255924 — Microsoft's ASN.1 library contains a memory management vulnerability that could be exploited by a remote attacker to cause a denial-of-service situation, or execute arbitrary code.

Note: Not all the vulnerabilities described in this Microsoft security update apply to Windows XPe on the I8800 I/Port, and are not listed in this Technical Bulletin.

RESOLUTION

To reduce the threat of these vulnerabilities, install this security update, along with these other updates:

- MS04-011
- MS04-028
- MS04-032

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