Topic: **I8800 I/Port Update: Sasser Virus Scanner**
Component(s) Affected: **I8800 I/Port**
Date: **February 15, 2005**

OVERVIEW / ENVIRONMENT

A new I/Port update file provides a scanner to locate and remove the Sasser virus from the I8800 I/Port.

Note: This update applies to the I8800 I/Port only.

DETAILED DESCRIPTION

Several new I/Port update files have been developed to enhance features and improve security on the I8800 I/Port. This Technical Bulletin details the following update:

Sasser Patch (Windows-KB841720-ENU-V4): This update scans for and deletes all instances of Sasser. Sasser is 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**. This worm can affect all unpatched machines running Windows XP or Windows 2000 connected to the Internet without a firewall. (*Source: F-Secure*).

A similar update is available for the Berbew virus, which is a Trojan horse program capable of stealing passwords from a compromised computer. See *Technical Bulletin TB0094MH, I8800 I/Port Update: Berbew Virus Scanner*.

Two sets of files are provided for each I/Port update:

- The local installer, in a folder named **Stand Alone**.
  - `Windows-KB841720-ENU-V4.exe`
- The Grid Center remote installer, in a folder named **GC Push**.
  - `UpdateSasser.bat`
  - `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.

TO APPLY UPDATE LOCALLY:

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. Turn off the Write Filter by double-clicking the **Write Filter Disable** icon on the desktop. The Write Filter is a special mechanism that prevents unauthorized writes to the I/Port's flash memory. The Write Filter sta-

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

tus is always displayed in the toolbar by a green circle for Write Filter Enabled (flash memory cannot be written), or by a red circle for Write Filter Disabled (flash memory can be written).

4. Insert the USB storage device into an available USB port.

5. Copy the installer file to C:\.

6. Double-click the installer file. The update installs automatically and reboots the I/Port.

Note: Do not press any keys during the update. Allow it to run undisturbed.

7. Delete the installer file from C:\ and double-click the Enable Write Filter icon to re-enable the Write Filter.

8. When the Write Filter has been re-enabled (a green circle is displayed in the tool bar), log out from the Administrator account.

TO APPLY THE UPDATE REMOTELY USING GRID CENTER:

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 Update file, including the .zip suffix (you can browse for this).

5. Enter the path and name of the Answer file, including the .bat suffix (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