Topic: **Eon e100 XPe Update: Microsoft Security Update – October 2005**
Component(s) Affected: **Eon e100 I/Port, XPe**
Date: **November 8, 2005**

OVERVIEW / ENVIRONMENT

ClearCube has provided a new I/Port update file to improve security on the Eon e100 I/Port running the Microsoft XPe operating system. This update comprises the following Microsoft Security Updates:

- MS05-045
- MS05-046
- MS05-047
- MS05-048
- MS05-049
- MS05-050
- MS05-051
- MS05-052

as they apply to Eon e100 XPe I/Port devices.

Microsoft Security Updates MS05-050 and MS05-052 are rated by Microsoft as critical updates.MS05-050 replaces MS03-030. Microsoft Security Updates MS05-046, MS05-047, MS05-049, and MS05-051 are rated by Microsoft as important updates. MS05-047 replaces MS05-039, discussed in *Technical Bulletin TB0158JS*. Microsoft Security Updates MS05-045 and MS05-048 are rated by Microsoft as moderate updates for Windows XP.

This update package should be considered a critical update. It is available on the ClearCube Technology Support website as `E100_XPe_October_2005_Hotfix_Snap-in.zip`.

For a summary of Microsoft security updates for Eon e100 I/Ports, please see *Technical Bulletin TB0159, Summary of Eon e100 XPe Security Updates*. For a summary of other updates for Eon e100 I/Ports, please see *Technical Bulletin TB0161, Cumulative List of Updates for Eon e100 I/Ports*.

Note: This update applies to the Eon e100 I/Port only. Do not attempt to install this on other devices. ezRemote Manager software is required to install this snap-in. For a summary of Microsoft security updates for I8800 I/Ports, please see *Technical Bulletin TB0096JS, Summary of I8800 I/Port Security Updates*.

DETAILED DESCRIPTION

This vulnerability is addressed in MS05-045:

http://www.microsoft.com/technet/Security/bulletin/ms05-045.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2307 — A denial of service vulnerability exists in the Network Connection Manager. An attacker who successfully exploited this vulnerability could cause the component responsible for managing network and remote access connections to stop responding. If the affected component is stopped due to an attack, it automatically restarts when new requests are received.

An attacker must have valid logon credentials to exploit this vulnerability. The vulnerability could not be exploited by anonymous users. However, remote authenticated users could attempt to exploit this vulnerability. In certain configurations, anonymous users could authenticate as the Guest account.

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

This vulnerability is addressed in MS05-046:

http://www.microsoft.com/technet/Security/bulletin/ms05-046.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1985 — A remote code execution vulnerability exists in the Client Service for NetWare (CSNW). An attacker who successfully exploited this vulnerability could remotely 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. By default, CSNW is not installed on any affected operating system version. Only customers who manually installed CSNW could be vulnerable to this issue. Listed as “Important” update.

Note: By default, the Client Service for NetWare is not installed on any affected operating system version. Only customers who manually install this service are likely to be vulnerable to this issue.

This vulnerability is addressed in MS05-047:

http://www.microsoft.com/technet/Security/bulletin/ms05-047.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2120

http://www.kb.cert.org/vuls/id/214572 — A remote code execution vulnerability exists in Plug and Play (PnP) that could allow an authenticated attacker to take complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. An attacker must have valid logon credentials to try to exploit this vulnerability. The vulnerability could not be exploited remotely by anonymous users. However, the affected component is available remotely to users who have standard user accounts.

This vulnerability is similar to the issue reported in MS05-039 **http://www.kb.cert.org/vuls/id/998653**. However, the issue reported in MS05-047 **http://www.kb.cert.org/vuls/id/214572** is only exploitable by local, authenticated users on Windows XP SP2. This security update replaces MS05-039.

Proof-of-concept exploit code has been made public, with the implication that this is being exploited.

This vulnerability is addressed in MS05-048:

http://www.microsoft.com/technet/Security/bulletin/ms05-048.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1987

http://www.us-cert.gov/cas/techalerts/TA05-284A.html

An unchecked buffer in Collaboration Data Objects (CDO), as used in Microsoft Windows and Microsoft Exchange Server, could allow remote attackers to execute arbitrary code when CDOSYS or CDOEX processes an e-mail message with a large header name. An attacker who successfully exploited this vulnerability could take complete control of the affected system, then install programs; view, change, or delete data; or create new accounts with full user rights.

These vulnerabilities are addressed in MS05-049:

http://www.microsoft.com/technet/Security/bulletin/ms05-049.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2117

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2118

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2122

http://www.us-cert.gov/cas/techalerts/TA05-284A.html — Multiple vulnerabilities in the Windows Shell could allow remote code execution. If a user is logged on with administrative user rights, 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. However, user interaction is required to exploit this vulnerability. For a more detailed description of the issues described in TA05-284A, please see *Technical Bulletin TB0171: I/Port I8800: Microsoft Security Update MS05-052*.

This vulnerability is addressed in MS05-050:

http://www.microsoft.com/technet/Security/bulletin/ms05-050.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2128

http://www.kb.cert.org/vuls/id/995220 — A remote code execution vulnerability exists in DirectShow (part of Windows Media Player 9) that could allow an attacker who successfully exploited this vulnerability to gain the same user rights as the local user. 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. This security update replaces MS03-030.

Note: DirectX is not installed in the e100 XPe factory system image.

These vulnerabilities are addressed in MS05-051:

http://www.microsoft.com/technet/Security/bulletin/ms05-051.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2119

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1978

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1979

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1980

http://www.kb.cert.org/vuls/id/950516

http://www.kb.cert.org/vuls/id/180868 — A range of vulnerabilities in Microsoft Distributed Transaction Coordinator (MSDTC), COM+, and Transaction Internet Protocol (TIP) could allow an attacker to 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.

Some of the COM+ vulnerabilities are similar to the vulnerabilities listed in http://www.us-cert.gov/cas/techalerts/TA05-284A.html and addressed by Microsoft Security Update MS05-052. Readers are advised to see Microsoft Knowledge Base Article 909444 at http://support.microsoft.com/kb/909444 as it applies to Windows XP before installing this update.

This vulnerability is addressed in MS05-052:

http://www.microsoft.com/technet/Security/bulletin/ms05-052.mspx

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2127

http://www.us-cert.gov/cas/techalerts/TA05-284A.html — The Microsoft DDS Library Shape Control (Msdds.dll) and other COM objects in Internet Explorer could be incorrectly instantiated, allowing an attacker to take complete control of an affected system. If a user is logged on with administrative user rights, 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 would be less impacted than users who operate with administrative user rights.

MS05-052 replaces MS05-037 and MS05-038, not previously incorporated in a security update for the e100 XPe I/Port.

RESOLUTION

To reduce the threat of these vulnerabilities, install this security update. This update is provided in a zipped file containing this Technical Bulletin and the updater install wizard. The updater install wizard is an executable file that installs the update package into the ezRemote Manager update folder.

To install this update with ezRemote Manager, do the following:

1. Download the patch file, which contains the update install wizard and this Technical Bulletin, and unzip it.

2. Load the install wizard file onto a Mass Storage Device (MSD) such as a key drive.
3. Copy the file to the ezRemote Manager console, and run the install wizard. It installs the necessary update files into the `\\Neoware\XPE\Snapins\` directory, in a folder identified by the month and year of the update.
4. Start ezRemote Manager.
5. From the list of discovered XPe Eon e100s, select the units to be updated.
6. Click the **Snapins** button in the top menu bar.
7. Browse to the update directory and select the `Install.2do` file. Click **OK**.
8. Click **OK** again to install the security update.

Note: Security updates must be installed in chronological order. For a summary of Microsoft security updates for e100 XPe I/Ports, please see *Technical Bulletin TB0159, Summary of Eon e100 XPe Security Updates*. For a summary of Microsoft security updates for I8800 I/Ports, please see Technical Bulletin TB0096, *Summary of I8800 I/Port Security Updates*.

For summaries of other I/Port updates, please see Technical Bulletin TB0161, *Cumulative List of Updates for Eon e100* and Technical Bulletin TB0162, *Cumulative List of Updates for I8800 I/Ports*.

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