**Topic:** **Eon e100 XPe Update: Microsoft Security Update – June 2005**
**Component(s) Affected:** **Eon e100 I/Port, XPe**
**Date:** **August 23, 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 Microsoft Security Updates MS05-025, MS05-026, MS05-028, and MS05-032 for Windows XPe as it applies to Eon e100 I/Port devices. This update addresses a number of vulnerabilities, as listed in this Technical Bulletin.

MS05-025 is a cumulative update that replaces MS05-020. MS05-026 replaces MS03-044, MS04-023, and MS05-001. Those updates have already been incorporated into the Eon e100 base system image.

Microsoft Security Updates MS05-025 and MS05-026 are rated by Microsoft as critical updates. Microsoft Security Update MS05-028 is rated by Microsoft as an important update. Microsoft Security Update MS05-032 is rated by Microsoft as a moderate updates. This update package should be considered a critical update.

**Note:** This update applies to the Eon e100 I/Port only. Do not attempt to install this on other devices.

## DETAILED DESCRIPTION

These vulnerabilities are addressed in MS05-025:
http://www.microsoft.com/technet/security/Bulletin/MS05-025.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1211
http://www.kb.cert.org/vuls/id/189754 — A buffer overflow in the Portable Network Graphics (PNG) image rendering component of Microsoft Internet Explorer (IE) may allow a remote attacker to execute code on a vulnerable system. The PNG image format is used as an alternative to other image formats such as the Graphics Interchange Format (GIF). IE supports the PNG image format. The PNG image rendering component of IE (`pngfilt.dll`) does not properly handle PNG image files, potentially allowing a buffer overflow to occur. If a remote attacker can persuade a user to access a specially crafted PNG image with IE, that attacker may be able to trigger the buffer overflow.

If a user is logged on with administrative user rights, an attacker successfully exploiting this vulnerability could 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. 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.

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0648
An information disclosure vulnerability exists in Internet Explorer because of the way that it handles certain requests to display XML content. An attacker could exploit this vulnerability by constructing a malicious Web page that could potentially lead to information disclosure if a user visited this site or viewed a malicious e-mail message. An attacker who successfully exploited this vulnerability could read XML data from another Internet Explorer domain. However, user interaction is required to exploit this vulnerability.

This vulnerability is addressed in MS05-026:
http://www.microsoft.com/technet/security/Bulletin/MS05-026.mspx
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1208
http://www.kb.cert.org/vuls/id/851869 — An integer overflow vulnerability exists in the Microsoft HTML Help system that could allow remote code execution on an affected system. HTML Help is the standard help system for the Windows platform. HTML Help components can be compiled to compress HTML,

graphic, and other files into a relatively small `.chm` compiled help file. The resulting `.chm` file can then be distributed with a software application or downloaded from the Web. The Help Viewer application uses the underlying components of Microsoft Internet Explorer to display help content.

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. Users whose accounts are configured to have fewer user rights on the system are less impacted than users who operate with administrative user rights.

This vulnerability is addressed in MS05-028:
**http://www.microsoft.com/technet/security/Bulletin/MS05-028.mspx**
**http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1207**
A buffer overflow in the Web Client service in Microsoft Windows XP allows remote authenticated users to execute arbitrary code via a crafted WebDAV request containing special parameters. An attacker who successfully exploited this vulnerability could 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.

This vulnerability is addressed in MS05-032:
**http://www.microsoft.com/technet/security/Bulletin/MS05-032.mspx**
A vulnerability in Microsoft Agent could enable a remote attacker to spoof trusted Internet content and execute arbitrary code by disguising security prompts on a malicious Web page. This can be exploited to trick a user into believing that they are looking at trusted content when actually visiting a malicious web site. Successful exploitation requires that a user visits a malicious web site.

## 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 Eon e100 XPes, 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 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 |