TheBillyGoatCurse.com

Limbo CMS XSS, Session Riding Multiple Vulnerabilities

Release date: December 27th, 2004

Date Discovered: December 18th, 2004

Severity: Highly Critical

Vendor: Limbo - Lite Mambo (http://mamboforge.net/projects/limbo/)

Impact: Cross Site Scripting w. Session Riding
Remote System Access

Vulnerable Software: Limbo v1.0.2

Overview:

Limbo CMS v1.0.2 does not properly check for malformed input in multiple core functions of the Content Management System. This lack of input sanitation creates a vulnerable state that allows potential attackers to inject scripts within core functions of Limbo.

Limbo uses cookies for administrative authorization access control, allowing cross site scripting (XSS) type attacks to be used to steal admin passwords. Limbo also has a file manager module installed by default, which can be exploited by a session riding attack when used in tandem with a XSS attack. This combination attack allows an attacker to place a file (I.E. PHP script, defacement, password phishing page) compromising the server and exploiting visitors to the compromised site.

This attack is further assisted by a XSS attack that can cause scripts to run in the administrative section of Limbo, denying the admin the ability to remove the malicious files and restore the site to an unowned status.

Solution:
Sanitize user input to strip HTML, Java Script and other unnecessary characters, or upgrade to latest version of Limbo.

Vendor Solution:
A patch/upgrade is available to provide sanitization of user input.

Vendor Status:
Limbo v1.0.3 alpha is available from http://mosforge.net

Credits:
Ryan McGeehan - Ryan at TheBillyGoatCurse dot com
Greetz to pd

Disclaimer
The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are no warranties, implied or express, with regard to this information. In no event shall the author be liable for any direct or indirect damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.