security-assessment.com

Vulnerability Advisory

Name	Cart32 Arbitrary File Download
Date Released	October 04, 2007
Affected Software	All releases prior to and including v6.3
Researcher	Paul Craig paul.craig@security-assessment.com

Description

Security-Assessment.com has discovered a highly critical vulnerability within the Cart32 administrative application. The vulnerability allows
a remote unauthenticated user to arbitrarily download any file present on the same physical disk that Cart32 is installed on.

The vulnerability stems from a NULL byte injection flaw within a file read function.

Exploitation

The function GetImage, part of c32web.exe displays various images from a supplied “ImageName” variable.
Example: http://host.com/scripts/c32web.exe/GetImage?ImageName=test.gif
C32web.exe attempts to prevent arbitrary files from being disclosed by only displaying files with an extension of .jpg, .gif, .png and .pdf.
Any file, of any extension type can be downloaded when a NULL byte is injected into the ImageName variable with a valid file extension suffixed directly after.

Example
http://host.com/scripts/c32web.exe/GetImage?ImageName=somefile.txt%00.gif
http://host.com/scripts/c32web.exe/GetImage?ImageName=somefile.txt%00.jpg
http://host.com/scripts/c32web.exe/GetImage?ImageName=somefile.txt%00.pdf
http://host.com/scripts/c32web.exe/GetImage?ImageName=somefile.txt%00.png

This vulnerability can be used to read any file on disk, including the Cart32 database file.

Solution

A new build of Cart32 v6.4 is available to address this vulnerability.
Security-Assessment.com highly recommends all Cart32 users to upgrade.

About Security-Assessment.com

Security-Assessment.com is Australasia’s leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs.
For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093