security-assessment.com

Vulnerability Advisory

Name	SiteKiosk - FileSystem Access
Vendor Website	http://www.sitekiosk.com/
Date Released	December 12, 2006
Affected Software	SiteKiosk < 6.5.150
Researcher	Brett Moore brett.moore@security-assessment.com

Overview

SiteKiosk is an application used to secure public access terminals. It is designed to provide a safe and stable way for the use of public access terminals with or without access to the Internet.

SiteKiosk is based on Internet Explorer and can be configured to individually restrict access to Web sites, the operating system, system settings, and applications. Your computer will be protected against any manipulation from the time you boot until you shut it down.

SiteKiosk suffers from a cross site scripting vulnerability, that leads to filesystem access.

Exploitation

SiteKiosk implements a 'skinning' feature so that the layout and display of the browser can be modified. The 'skinning' feature uses an HTML aware control for the modified title bar of the main SiteKiosk window.

SiteKiosk displays the URL of the current location in the title bar of the main window, and therefore any HTML code in the location will be included in the title bar.

By default, SiteKiosk does not properly handle the ABOUT: prefix. The URL is directly outputted to the screen leading to a normal cross site scriptingvulnerability.

Because the URL is also outputted to the title bar, script can be executedunder the LOCAL computer zone.

If a user types the following into the address box, or browses a site that sets the location to;

```
        ABOUT:hello<a href=\>click here</a>
```

The title bar will display a hyperlink. By clicking on this HREF in the main windows title bar, the filesystem will be accessed with an explorerwindow.

SiteKiosk also installs some activeX controls that are marked 'safe for scripting'. One of these controls exposes two dangerous methods that allow a SiteKiosk user to read and download any file from the kiosk with the permissions of the user running SiteKiosk.

Solutions

A new version of SiteKiosk has been released that addresses these vulnerabilities. It can be downloaded from http://www.sitekiosk.com.

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

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