security-assessment.com

Vulnerability Advisory

Name	StoryBoard Quick 6 Stack Buffer Overflow
Vendor Website	http://www.powerproduction.com/
Date Released	29/11/2011
Affected Software	StoryBoard Quick 6 (potentially also StoryBoard Artist and StoryBoard Studio)
Researcher	Nick Freeman (nick.freeman@security-assessment.com)

Description

Security-Assessment.com has discovered a file format vulnerability in the XML files used to describe frames in the StoryBoard Quick 6 software. The <string> element used to define a filename was found to be vulnerable to a buffer overflow, which can be exploited to execute arbitrary code under the context of the user running StoryBoard Quick 6. Supplying a long file name causes memory corruption within the application.

By crafting a file that contains more than 507 characters in the <string> field, the StoryBoard Quick 6 application will use the next 4 characters in an unsafe manner. These four characters are used as a pointer to the source address for a string copy function. It is possible to write user-supplied data onto the stack by changing the value of these 4 characters to a memory location containing a pointer to data within the Frame.xml file. This strcpy function overwrites a significant portion of the stack, including the Structured Exception Handler.

Exploitation

A proof of concept exploit for this vulnerability can be found on the Security-Assessment.com website at http://security-assessment.com/files/storyboardquick6poc.zip. A Metasploit module can be found at http://security-assessment.com/files/storyboardquick6.rb. This proof of concept exploit has been tested on the latest build of Windows XP SP3, and does not bypass DEP.

Solution

No known patch is available at this time.

Disclosure Timeline

Security-Assessment.com practices responsible disclosure and made significant effort to report this vulnerability to PowerProduction Software.

13/06/2011: First email sent to PowerProduction, asking for contact details for security or developer personnel.
17/06/2011: After several attempts to get in contact, PowerProduction asks me for a customer number.
17/06/2011: Security-Assessment.com replies stating that this issue is exploitable without a customer number. No response was received from PowerProduction after this email.
23/06/2011: Security-Assessment.com sends a follow-up email stating that the vulnerability is still present.
10/07/2011: A final email is sent stating that PowerProduction customers are vulnerable.
05/11/11: Vulnerability released at Kiwicon V in Wellington, New Zealand.
19/11/11: Vulnerability released at Ruxcon 2011 in Melbourne, Australia.
29/11/11: Vulnerability advisory and exploit code published.

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.