security-assessment.com

Vulnerability Advisory

Name	Final Draft 8 Multiple Stack Buffer Overflows
Vendor Website	http://www.finaldraft.com/index.php
Date Released	29/11/2011
Affected Software	Final Draft < 8.02
Researcher	Nick Freeman (nick.freeman@security-assessment.com)

Description

Security-Assessment.com has discovered several file format vulnerabilities in .fdx and .fdxt files, as used by the script writing software, Final Draft 8.

The following XML tag elements were found to be vulnerable to buffer overflows, which can be exploited to execute arbitrary code under the context of the user running Final Draft 8:

<Word> in <IgnoredWords>
<Transition> in <SmartType>
<Location> in <SmartType>
<Extension> in <SmartType>
<SceneIntro> in <SmartType>
<TimeOfDay> in <SmartType>
<Character> in <SmartType>

By crafting a file that contains more than 10,032 characters in one of the above fields, the Final Draft 8 application will crash as a result of a buffer overflow overwriting the SEH (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/finaldraft8poc.zip. A Metasploit module can be found at http://security-assessment.com/files/finaldraft8.rb. This proof of concept exploit has been tested on the latest build of Windows XP SP3, and does not bypass DEP.

Solution

The latest version of Final Draft (version 8.02) remediates this vulnerability. This can be downloaded from the Final Draft website.

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.

Copyright Security-Assessment.com 2011