security-assessment.com

Vulnerability Advisory

Name	Mozilla Firefox 'shlwapi.dll' Use-after-free
Vendor Website	http://www.mozilla.org/
Date Released	14/03/2012 - CVE-2012-0454
Affected Software	Mozilla Firefox < 11 (32-bit Windows 7)
Researchers	Scott Bell & Blair Strang

Description

Mozilla Firefox prior to version 11 on 32-bit Windows 7 is vulnerable to memory corruption in the way it handles file open dialogues.

It is possible to cause a use-after-free condition by spawning a child window which uses the file picker dialogue window, and then closing the child window.

Exploitation

Exploitation of this vulnerability requires a user running a vulnerable version of Mozilla Firefox to visit a page containing specially crafted JavaScript. Users can generally be lured to visit web pages via email, instant message or links on the internet. Successful exploitation of this vulnerability will result in a remote user gaining code execution under the context of the Firefox process.
This vulnerability will be demonstrated at Hack in The Box Amsterdam 2012 later this year.

Solution

This vulnerability has been fixed in Mozilla Firefox 11. Security-Assessment.com recommends updating to the latest version provided by the vendor.

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.

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 +64 4 472 5093

dimension data