security-assessment.com

Vulnerability Advisory

Name	Internet Explorer SLayoutRun Use After Free Vulnerability
Vendor Website	http://www.microsoft.com/
Date Released	14/02/2013
Affected Software	Microsoft Internet Explorer 8
Researchers	Scott Bell

Description

A Use-after-free memory corruption vulnerability was identified in Microsoft Internet Explorer 8. This allows a malicious user to remotely execute arbitrary code on a vulnerable user's machine, in the context of the current user.

The memory corruption happens when the application of a style sheet performs style computations on the DOM. A CParaElement node is released but a reference is still kept in CDoc. This memory is reused when a CDoc relayout is performed.

Exploitation

Exploitation of this vulnerability requires a user 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. Vulnerabilities like this are often hosted on legitimate websites which have been compromised by other means.

Due to the inability to dynamically create an object while still triggering the vulnerability, a clean vtable overwrite was not possible. To exploit this vulnerability a 'pray-after-free' approach was taken. This approach works by filling memory with incremental sized blocks in the hope that an allocation of the correct size will be placed into the memory location of the freed object. Below is a Metasploit module which exploits this vulnerability:

Metasploit exploit module
http://www.security-assessment.com/files/documents/advisory/ms13_009_ie_slayoutrun_uaf.rb

Solution

Microsoft validated this security issue in Internet Explorer 8 and issued a patch (MS13-009) to remedy it. Security-Assessment.com recommends applying the patch which has been made available via Windows Update.

About Security-Assessment.com

Security-Assessment.com is a 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 4 460 2596