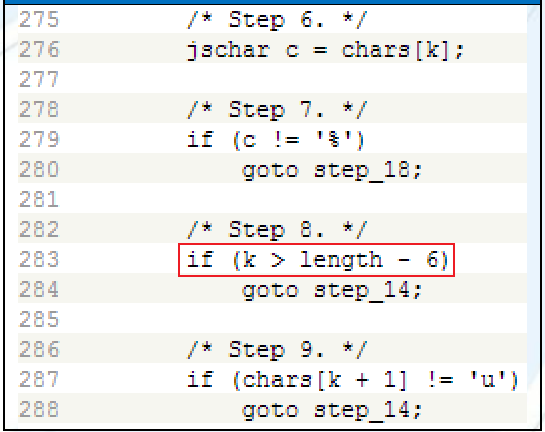
Vulnerability Advisory

Name	Mozilla ‘str_unescape’ Heap Overflow
Vendor Website	http://www.mozilla.org/
Date Released	21/11/2012
Affected Software	Firefox, Thunderbird, SeaMonkey
Researchers	Scott Bell

Description

The Mozilla JavaScript engine is vulnerable to a heap overflow vulnerability in the way the JavaScript engine’s unescape function processes strings. This is due to an integer underflow when the string length is less than 6 characters, as shown in the code snippet below:

Vulnerable code

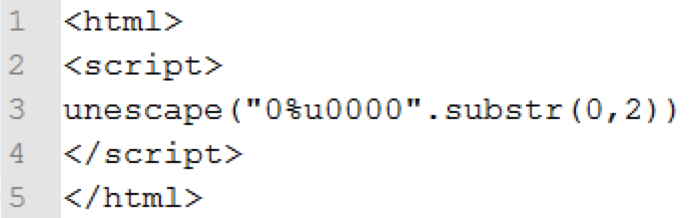


```
    /* Step 6. */
    jschar c = chars[k];

    /* Step 7. */
    if (c != '%')
        goto step_18;

    /* Step 8. */
    if (k > length - 6)
        goto step_14;

    /* Step 9. */
    if (chars[k + 1] != 'u')
        goto step_14;
```

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. The following HTML proof of concept code can be used to reproduce the vulnerability in Mozilla Firefox:

Proof of concept HTML



```
<html>
<script>
unescape("0%u0000".substr(0,2))
</script>
</html>
```

Solution

This vulnerability is fixed in Mozilla Firefox and Thunderbird version 17. Security-Assessment.com recommends updating to the latest version provided by the vendor.

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 9 302 5093