LIONIC®
Security Chip Provider

31/05/2011
Doc No: SN-2011-22007

Security News
2011-22007 Adobe Audition Session File Handling Buffer Overflow Vulnerability

1. Affected Version

Adobe Audition 3.0.1 and earlier versions for Windows

2. Description

A buffer overflow vulnerability has been identified in Adobe Audition 3.0.1 and earlier versions for Windows. This flaw allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Audition Session (aka .ses) file.

3. Vulnerability Analysis

The partial malicious content is listed as follows:

```
$data = "\x43\x4F\x4F\x4C\x4E\x45\x53\x53\x50\xF2\x08\x00"
    "\x68\x64\x72\x20\xF0\x03\x00\x00\x22\x56\x00\x00"
    "\xFC\x17\x0A\x00\x00\x00\x00\x00\x20\x00\x01\x00"
    "\x00\x00\x00\x00\x00\x00\xF0\x3F\x00\x00\x00\x00"
    "\x00\x00\xF0\x3F\x41\x41\x41\x41\x41\x41\x41\x41"
    "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41"
    "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41"
    "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41"
    "\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41\x41"
```

Table 1: The partial malicious content

Adobe Audition fails to properly sanitize user input, resulting in memory corruption, overwriting memory registers which may lead to arbitrary code execution or denial of service. An attacker would need to convince a user to open a malicious binary Audition Session (.ses) file to successfully exploit the issue.

Per Adobe Security Bulletin: *The Audition Session (.ses) file format is an older format that is no longer supported with the release of Adobe Audition CS5.5.*

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 19/05/2011.
2. Apply the appropriate patch for your system, as listed in Adobe Security advisory.
3. Adobe strongly recommends Audition users discontinue use of the Adobe Session (.ses) file format and switch to use of the XML session format. XML is a human-readable standard for electronically encoding documents with numerous benefits over binary formats. With the release of Audition CS5.5, the binary Audition Session (.ses) file format is no longer supported.

5. Reference

1. http://www.adobe.com/support/security/bulletins/apsb11-10.html
2. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0614