LIONIC®
Security Chip Provider

01/19/2011
Doc No: SN-2011-03002

Security News
2011-03002 ActiveX UserManager 2.03 Buffer Overflow Vulnerability

1. Affected Version

ActiveX UserManager 2.03

2. Description

1. ActiveX usermanager is a free software which is a COM interface to Windows NT/2000/XP local or domain account database.

2. There is a vulnerability found in method “SelectServer” 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:E5D2CE27-5FA0-11D2-A666-204C4F4F5020' id='target'></object>
<script language='vbscript'>
arg1=String(1044, "A")
arg2=True
exploit = arg1
target.SelectServer exploit ,arg2
</script>
```

Table 1: The proof-of-concept code

In the above of PoC, it sends lots of characters “A” to the method “SelectServer”. The first parameter of method “SelectServer” is a Server name and the second is a Boolean value to set if using filter. When receiving lots of characters in parameter, it couldn't be handled correctly. This PoC would cause this tool crash. If the attacker injects malicious shellcode, the computer would be infected automatically when visits this crafted web pages.

4. Recommendation

1. Lionic IDP signature database can prevent this attack since 01/19/2011.

5. Reference

1. http://www.brothersoft.com/activex-usermanager-14519.html
2. http://packetstormsecurity.org/files/view/97573/usermanager-overflow.txt