

[NEWS] OpenVPN foreign_option() Formart String

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0020.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/06/05

To: list@securiteam.com

Date: 6 Nov 2005 13:34:51 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

OpenVPN foreign_option() Formart String

SUMMARY

" <<http://openvpn.net/>> OpenVPN is a full-featured SSL VPN solution which can accomodate a wide range of configurations, including remote access, site-to-site VPNs, WiFi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access-controls."

OpenVPN contains a remotely exploitable format string vulnerability in the way it processes command-line/config arguments.

DETAILS

Vulnerable Systems:

- * OpenVPN version 2.0 up to 2.0.3

Immune Systems:

- * OpenVPN version 2.0.4

The vulnerable function is located in options.c in the foreign_option() function. This function uses the buf_printf() function to improperly write to a buffer(typical printf() format string-style). The only option that appears to use the foreign_option() function is "dhcp-option".

Securiteam: [NEWS] OpenVPN foreign_option() Formart String

Since the OpenVPN server is allowed to "push" some command options ("dhcp-option" being one of those) to its clients this becomes remotely exploitable on the OpenVPN clients. An example/demonstration of this would be to insert the following line into a malicious OpenVPN server config file:

```
push "dhcp-option <format string>"
```

Or, namely to test for validity/crash of an OpenVPN client:

```
push "dhcp-option %n%n%n%n%n%n"
```

It should be noted that WIN32 versions of OpenVPN are NOT affected by this, the following code snippets will highlight the above.

openvpn/options.c:

```
..
static void foreign_option (struct options *o, char *argv[], int len,
struct env_set *es)
{
    if (len > 0)
    {
        struct gc_arena gc = gc_new();
        struct buffer name = alloc_buf_gc (OPTION_PARM_SIZE, &gc);
        struct buffer value = alloc_buf_gc (OPTION_PARM_SIZE, &gc);
        int i;
        bool first = true;

        buf_printf (&name, "foreign_option_%d", o->foreign_option_index +
1);
        ++o->foreign_option_index;
        for (i = 0; i < len; ++i)
        {
            if (argv[i])
            {
                if (!first)
                    buf_printf (&value, " ");
                !-> buf_printf (&value, argv[i]);
                first = false;
            }
        }
        setenv_str (es, BSTR(&name), BSTR(&value));
        gc_free (&gc);
    }
}

..

static int add_option (...){
..
#ifdef WIN32
```

```
..
#else
..
  else if (streq (p[0], "dhcp-option") && p[1])
  {
    ++i;
    VERIFY_PERMISSION (OPT_P_IPWIN32);
    if (p[2])
      ++i;
! -> foreign_option (options, p, 3, es);
  }
..
#endif
..
```

User-supplied data is reachable for writing to, and addresses (within pop/"direct parameter access" range) already in memory were viable to write and to gain control of the program. However, OpenVPN filters many characters, which causes problems for standard exploitation using the user supplied method and insertion of (non-alum) shellcode. this does not stop exploitation using this method, but does make it more involved.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-3393>>
CVE-2005-3393

ADDITIONAL INFORMATION

The information has been provided by <mailto:v9@fakehalo.us> v9.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.