TheGreenBow IPSec VPN Client Login Credentials Information Disclosure Vulnerability

Informations

Risk: Low
Typology: Local
Date: 30/03/2008
Product: TheGreenBow IPSec VPN Client
Version: 4.10.010
Vendor: http://www.thegreenbow.com/vpn.html
Vendor Status: 29/03/2008 - Vendor Informed
Discovered By: Giuseppe `Evilcry` Bonfa'

Description

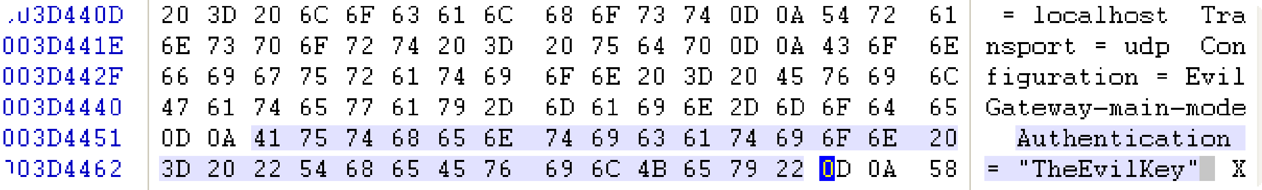
TheGreenBow IPSec VPN Client is an on demand IPSec VPN Client, compliant with most popular VPN gateways and with network tools to deploy security in large and medium enterprises. Highly efficient and easy to configure, the IPSec VPN Client also allows peer-to-peer VPN.

PoC

TheGreenBow IPSec VPN Client 4.10.010 is prone to a Login Credentials that could expose local users of TheGreenBow to a leak of Sensitive Informations, specifically an attacker could Carve, Login and Certificates used by the user, cause they are stored in clear in memory. This may lead complete User Impersonation.

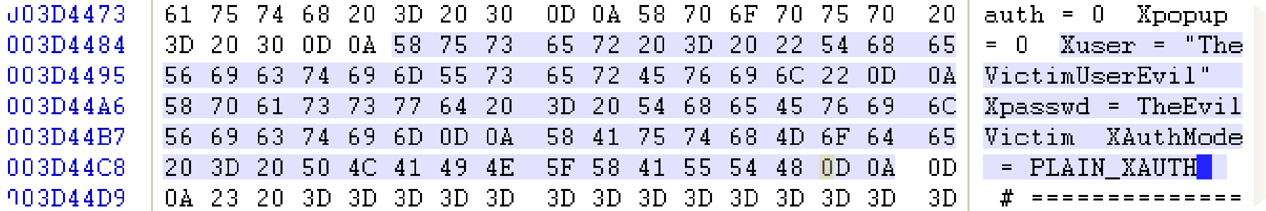
Attackers can exploit this issue to harvest VPN login credentials and gain unauthorized access to networks and resources protected by the VPN.

All informations are stored in the meomory image of the process 'Tgbike.exe', so with a basical Process Memory Dumper.



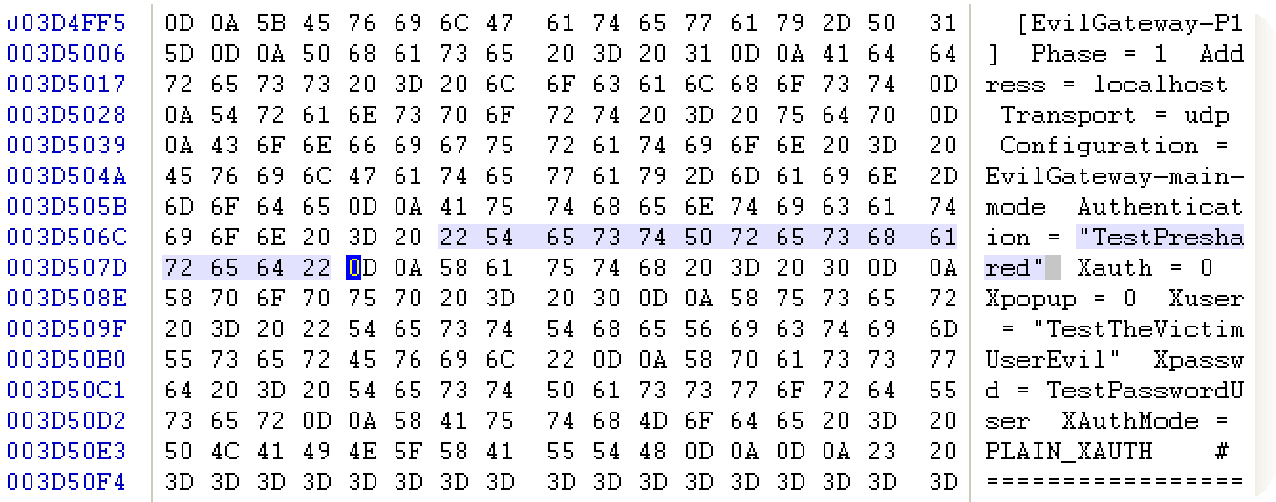
```
003D440D  20 3D 20 6C 6F 63 61 6C  68 6F 73 74 0D 0A 54 72  61   = localhost  Tra
003D441E  6E 73 70 6F 72 74 20 3D  20 75 64 70 0D 0A 43 6F  6E  nsport = udp  Con
003D442F  66 69 67 75 72 61 74 69  6F 6E 20 3D 20 45 76 69  6C  figuration = Evil
003D4440  47 61 74 65 77 61 79 2D  6D 61 69 6E 2D 6D 6F 64  65  Gateway-main-mode
003D4451  0D 0A 41 75 74 68 65 6E  74 69 63 61 74 69 6F 6E  20    Authentication
003D4462  3D 20 22 54 68 65 45 76  69 6C 4B 65 79 22 0D 0A  58  = "TheEvilKey"  X
```

Second Screenshot:



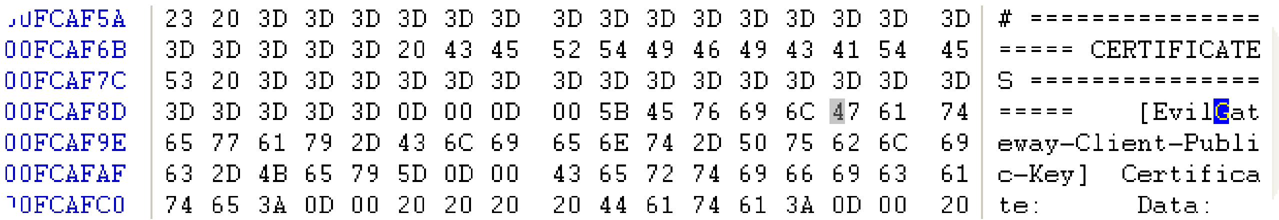
```
003D4473  61 75 74 68 20 3D 20 30  0D 0A 58 70 6F 70 75 70  20  auth = 0  Xpopup
003D4484  3D 20 30 0D 0A 58 75 73  65 72 20 3D 20 22 54 68  65  = 0  Xuser = "The
003D4495  56 69 63 74 69 6D 55 73  65 72 45 76 69 6C 22 0D  0A  VictimUserEvil"
003D44A6  58 70 61 73 73 77 64 20  3D 20 54 68 65 45 76 69  6C  Xpasswd = TheEvil
003D44B7  56 69 63 74 69 6D 0D 0A  58 41 75 74 68 4D 6F 64  65  Victim  XAuthMode
003D44C8  20 3D 20 50 4C 41 49 4E  5F 58 41 55 54 48 0D 0A  0D   = PLAIN_XAUTH
003D44D9  0A 23 20 3D 3D 3D 3D 3D  3D 3D 3D 3D 3D 3D 3D 3D  3D   # ==============
```

Global Shot:



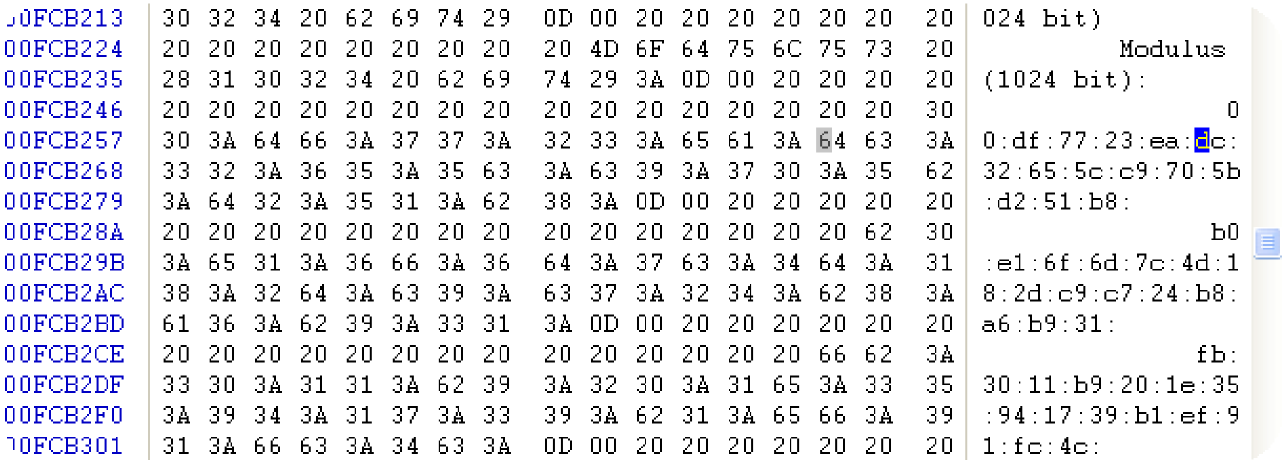
```
003D4FF5  0D 0A 5B 45 76 69 6C 47  61 74 65 77 61 79 2D 50  31    [EvilGateway-P1
003D5006  5D 0D 0A 50 68 61 73 65  20 3D 20 31 0D 0A 41 64  64  ]  Phase = 1  Add
003D5017  72 65 73 73 20 3D 20 6C  6F 63 61 6C 68 6F 73 74  0D  ress = localhost
003D5028  0A 54 72 61 6E 73 70 6F  72 74 20 3D 20 75 64 70  0D   Transport = udp
003D5039  0A 43 6F 6E 66 69 67 75  72 61 74 69 6F 6E 20 3D  20   Configuration =
003D504A  45 76 69 6C 47 61 74 65  77 61 79 2D 6D 61 69 6E  2D  EvilGateway-main-
003D505B  6D 6F 64 65 0D 0A 41 75  74 68 65 6E 74 69 63 61  74  mode  Authenticat
003D506C  69 6F 6E 20 3D 20 22 54  65 73 74 50 72 65 73 68  61  ion = "TestPresha
003D507D  72 65 64 22 0D 0A 58 61  75 74 68 20 3D 20 30 0D  0A  red"  Xauth = 0
003D508E  58 70 6F 70 75 70 20 3D  20 30 0D 0A 58 75 73 65  72  Xpopup = 0  Xuser
003D509F  20 3D 20 22 54 65 73 74  54 68 65 56 69 63 74 69  6D   = "TestTheVictim
003D50B0  55 73 65 72 45 76 69 6C  22 0D 0A 58 70 61 73 73  77  UserEvil"  Xpassw
003D50C1  64 20 3D 20 54 65 73 74  50 61 73 73 77 6F 72 64  55  d = TestPasswordU
003D50D2  73 65 72 0D 0A 58 41 75  74 68 4D 6F 64 65 20 3D  20  ser  XAuthMode =
003D50E3  50 4C 41 49 4E 5F 58 41  55 54 48 0D 0A 0D 0A 23  20  PLAIN_XAUTH    #
003D50F4  3D 3D 3D 3D 3D 3D 3D 3D  3D 3D 3D 3D 3D 3D 3D 3D  3D  =================
```

And now Certificates Sniffing:



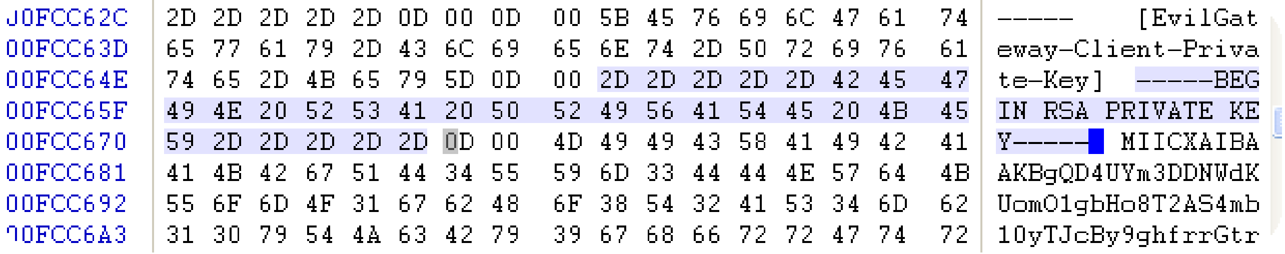
```
00FCAF5A  23 20 3D 3D 3D 3D 3D 3D  3D 3D 3D 3D 3D 3D 3D 3D  3D  # ===============
00FCAF6B  3D 3D 3D 3D 3D 20 43 45  52 54 49 46 49 43 41 54  45  ===== CERTIFICATE
00FCAF7C  53 20 3D 3D 3D 3D 3D 3D  3D 3D 3D 3D 3D 3D 3D 3D  3D  S ===============
00FCAF8D  3D 3D 3D 3D 3D 0D 00 0D  00 5B 45 76 69 6C 47 61  74  =====     [EvilGat
00FCAF9E  65 77 61 79 2D 43 6C 69  65 6E 74 2D 50 75 62 6C  69  eway-Client-Publi
00FCAFAF  63 2D 4B 65 79 5D 0D 00  43 65 72 74 69 66 69 63  61  c-Key]  Certifica
00FCAFC0  74 65 3A 0D 00 20 20 20  20 44 61 74 61 3A 0D 00  20  te:        Data:
```

Second Example



```
00FCB213  30 32 34 20 62 69 74 29  0D 00 20 20 20 20 20 20  20  024 bit)
00FCB224  20 20 20 20 20 20 20 20  20 4D 6F 64 75 6C 75 73  20           Modulus
00FCB235  28 31 30 32 34 20 62 69  74 29 3A 0D 00 20 20 20  20  (1024 bit):
00FCB246  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 20  30                  0
00FCB257  30 3A 64 66 3A 37 37 3A  32 33 3A 65 61 3A 64 63  3A  0:df:77:23:ea:dc:
00FCB268  33 32 3A 36 35 3A 35 63  3A 63 39 3A 37 30 3A 35  62  32:65:5c:c9:70:5b
00FCB279  3A 64 32 3A 35 31 3A 62  38 3A 0D 00 20 20 20 20  20  :d2:51:b8:
00FCB28A  20 20 20 20 20 20 20 20  20 20 20 20 20 20 20 62  30                 b0
00FCB29B  3A 65 31 3A 36 66 3A 36  64 3A 37 63 3A 34 64 3A  31  :e1:6f:6d:7c:4d:1
00FCB2AC  38 3A 32 64 3A 63 39 3A  63 37 3A 32 34 3A 62 38  3A  8:2d:c9:c7:24:b8:
00FCB2BD  61 36 3A 62 39 3A 33 31  3A 0D 00 20 20 20 20 20  20  a6:b9:31:
00FCB2CE  20 20 20 20 20 20 20 20  20 20 20 20 20 20 66 62  3A                fb:
00FCB2DF  33 30 3A 31 31 3A 62 39  3A 32 30 3A 31 65 3A 33  35  30:11:b9:20:1e:35
00FCB2F0  3A 39 34 3A 31 37 3A 33  39 3A 62 31 3A 65 66 3A  39  :94:17:39:b1:ef:9
00FCB301  31 3A 66 63 3A 34 63 3A  0D 00 20 20 20 20 20 20  20  1:fc:4c:
```

Private.key View:



```
00FCC62C  2D 2D 2D 2D 2D 0D 00 0D  00 5B 45 76 69 6C 47 61  74  -----     [EvilGat
00FCC63D  65 77 61 79 2D 43 6C 69  65 6E 74 2D 50 72 69 76  61  eway-Client-Priva
00FCC64E  74 65 2D 4B 65 79 5D 0D  00 2D 2D 2D 2D 2D 42 45  47  te-Key]  -----BEG
00FCC65F  49 4E 20 52 53 41 20 50  52 49 56 41 54 45 20 4B  45  IN RSA PRIVATE KE
00FCC670  59 2D 2D 2D 2D 2D 0D 00  4D 49 49 43 58 41 49 42  41  Y-----  MIICXAIBA
00FCC681  41 4B 42 67 51 44 34 55  59 6D 33 44 44 4E 57 64  4B  AKBgQD4UYm3DDNWdK
00FCC692  55 6F 6D 4F 31 67 62 48  6F 38 54 32 41 53 34 6D  62  UomO1gbHo8T2AS4mb
00FCC6A3  31 30 79 54 4A 63 42 79  39 67 68 66 72 72 47 74  72  10yTJcBy9ghfrrGtr
```

So we can identify some keywords to use for Credentials Carving:

```
Xuser = “”
Xpassword = “”
# ==================== CERTIFICATES ====================
-Client-Private-Key]
```