EXPLOIT_DB CHOICE

Name : Shriram Karpoora Sundara Pandian
Group : E (ECHO)
Course : Computer System Security

This vulnerability is associated with one of the most popular remote login providers, TPlus, and particularly happens on the Windows platform.

Like any other remote access provider like Citrix or Microsoft RD5, TPlus allows workers to remotely connect to office desktops to do their jobs securely and seamlessly from anywhere. It is a privilege given to the worker's but slowly turns into a threat for a company because of a lot of vulnerabilities.

The vulnerability I have attached can be visited at this link:

https://www.exploit-db.com/exploits/51679

How TPlus works and provides remote access to users is through the embedded web server they have, which manages and organises all the remotes connected to its central server and provides the necessary data in real time for their remote access.

However, a lot of insecure files and folders that have been present in the system can allow an attacker to make use of those files and change the credentials or try to escalate the privileges to himself, etc. These insecure files create a lot of noise and give an open backdoor for attackers, and those insecure files are:

```
C:\Program Files (x86)\TSplus\Clients\www
C:\Program Files (x86)\TSplus\Clients\www\addons
C:\Program Files (x86)\TSplus\Clients\www\ConnectionClient
C:\Program Files (x86)\TSplus\Clients\www\downloads
C:\Program Files (x86)\TSplus\Clients\www\prints
C:\Program Files (x86)\TSplus\Clients\www\RemoteAppClient
C:\Program Files (x86)\TSplus\Clients\www\software
C:\Program Files (x86)\TSplus\Clients\www\var
C:\Program Files (x86)\TSplus\Clients\www\cgi-bin\remoteapp
C:\Program Files (x86)\TSplus\Clients\www\downloads\shared
C:\Program Files (x86)\TSplus\Clients\www\software\java
C:\Program Files (x86)\TSplus\Clients\www\software\js
C:\Program Files (x86)\TSplus\Clients\www\software\html5\jwres
```

```
C:\Program Files (x86)\TSplus\Clients\www\software\html5\locales
C:\Program Files (x86)\TSplus\Clients\www\software\html5\imgs\topmenu
C:\Program Files
(x86)\TSplus\Clients\www\software\html5\imgs\key\parts
C:\Program Files (x86)\TSplus\Clients\www\software\java\img
C:\Program Files (x86)\TSplus\Clients\www\software\java\third
C:\Program Files (x86)\TSplus\Clients\www\software\java\img\cp
C:\Program Files (x86)\TSplus\Clients\www\software\java\img\srv
C:\Program Files (x86)\TSplus\Clients\www\software\java\third\images
C:\Program Files (x86)\TSplus\Clients\www\software\java\third\js

C:\Program Files

(x86)\TSplus\Clients\www\software\java\third\images\bramus
C:\Program Files
(x86)\TSplus\Clients\www\software\java\third\js\prototype
C:\Program Files (x86)\TSplus\Clients\www\var\log
C:\Program Files (x86)\TSplus\UserDesktop\themes
C:\Program Files (x86)\TSplus\UserDesktop\themes\BlueBar
C:\Program Files (x86)\TSplus\UserDesktop\themes\Default
C:\Program Files (x86)\TSplus\UserDesktop\themes\GreyBar
C:\Program Files (x86)\TSplus\UserDesktop\themes\Logon
C:\Program Files (x86)\TSplus\UserDesktop\themes\MenuOnTop
C:\Program Files (x86)\TSplus\UserDesktop\themes\Seamless
C:\Program Files (x86)\TSplus\UserDesktop\themes\ThinClient

C:\Program Files (x86)\TSplus\UserDesktop\themes\Vista
```

There are a lot of files, and another vulnerability of TPlus revolving around the remote connection is that they allow users to have a custom login page on the web server where they can store their credentials so that they don't need to re-enter the password to login to the new session. They can simply login with those saved credentials. This is convenient, right? But there is a problem there: the way the credentials are stored is silly because the credentials are stored in an insecure manner since they are saved in cleartext within the HTML login page.

This means that everyone with access to the web login page can easily retrieve the credentials to access the application by simply looking at the HTML code page.

This is how it looks if we access the web login page:

```
  // --------------- Access Configuration ---------------
   var user = "Admin";                          // Login to use when
connecting to the remote server (leave "" to use the login typed in
this
page)
```

```
   var pass = "SuperSecretPassword";           // Password to use
when
connecting to the remote server (leave "" to use the password typed
in
this page)
   var domain = "";                            // Domain to use when
connecting to the remote server (leave "" to use the domain typed in
this page)
   var server = "127.0.0.1";                   // Server to connect
to
(leave "" to use localhost and/or the server chosen in this page)
   var port = "";                              // Port to connect to
(leave "" to use localhost and/or the port of the server chosen in
this
page)
   var lang = "as_browser";                    // Language to use
   var serverhtml5 = "127.0.0.1";              // Server to connect
to,
when using HTML5 client
   var porthtml5 = "3389";                     // Port to connect to,
when using HTML5 client
   var cmdline = "";                           // Optional text that
will
be put in the server's clipboard once connected
   // --------------- End of Access Configuration ---------------
```

Link to that vulnerability :
https://www.exploit-db.com/exploits/51681

I chose these vulnerabilities because nowadays remote work seems to be a trend, and both companies and employees got used to that because of convenience and cost reductions to the company. With the growth of remote access providers, the chance of compromise in remote connections is very easy in some cases because of their product maturity and product cycle. In this case, TPlus has three remote vulnerabilities in their remote connections that can be exploited easily, and the chance of finding the new vulnerability is high.