

# SSD Advisory – TrendNet AUTHORIZED\_GROUP Information Disclosure

[blogs.securiteam.com/index.php/archives/3627](https://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.

```
phpcgi_main() func:
aPost_D:      .asciiz ".POST"<0> # DATA XREF: sub_405ACD+4C7c
              .align 2
aFiles:      .asciiz ".FILES"<0> # DATA XREF: sub_405ACD+847c
off_420798:   .word loc_412F4C+2 # DATA XREF: sub_405ACD+1147c
aFiletypes:  .asciiz ".FILETYPES"<0> # DATA XREF: sub_405ACD+1F47c
aGet_D:      .asciiz ".GET"<0> # DATA XREF: sub_405ACD+1647c
aServer:     .asciiz ".SERVER"<0> # DATA XREF: phpcgi_main+907c
aRequestMethod: .asciiz ".REQUEST_METHOD"<0>
              .align 2
aHead:      .asciiz ".HEAD"<0> # DATA XREF: phpcgi_main+1087c
aGet:       .asciiz ".GET"<0> # DATA XREF: phpcgi_main+1287c
aPost:     .asciiz ".POST"<0> # DATA XREF: phpcgi_main+1607c
ahtdocsWebInfoP: .asciiz "/htdocs/web/info.php"<0>
              .align 2
aInfoPhp:   .asciiz "/info.php"<0> # DATA XREF: phpcgi_main+1F47c
aFail:     .asciiz ".FAIL"<0> # DATA XREF: phpcgi_main+1F87c
aErrReqTooLong: .asciiz ".ERR_REQ_TOO_LONG"<0>
              .align 2
aUnsupportedHtt: .asciiz ".unsupported HTTP request"<0>
              .align 4
aAuthorizedGrou_D: .asciiz ".AUTHORIZED_GROUP"<0> # DATA XREF: phpcgi_main+25C7c
aSessionId:  .asciiz ".SESSION_UID"<0> # DATA XREF: phpcgi_main+29C7c
              .asciiz "
```

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

### Proof of Concept

```

main:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_405F28
    lui $a0, 0x40

loc_405F28:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_405F34
    lui $a0, 0x40

loc_405F34:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_406100
    lui $a0, 0x40

loc_405F28:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_405F34:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_406100:
    la $t9, sess_validate
    addiu $s0, $sp, 0x48+var_28
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, sprintf
    move $a2, $v0 # s
    move $a0, $a0 # s
    jalr $t9, sprintf # "AUTHORIZED_GROUP=%d"
    la $a1, aAuthorizedGroup_0 # "AUTHORIZED_GROUP=%d"
    move $a1, $a0
    la $t9, obj_add_string
    nop
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    move $a0, $a1
    la $t9, obj_add_char
    nop
    jalr $t9, obj_add_char
    li $a1, 0xA
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, obj_add_string
    la $a1, aSessionUid # "SESSION_UID="
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    nop
  
```

```

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 # s
    move $a0, $a0 # s
    jalr $t9, sprintf # "AUTHORIZED_GROUP=%d"
    la $a1, aAuthorizedGroup_0 # "AUTHORIZED_GROUP=%d"
    move $a1, $a0
    la $t9, obj_add_string
    nop
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    move $a0, $a1
    la $t9, obj_add_char
    nop
    jalr $t9, obj_add_char
    li $a1, 0xA
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, obj_add_string
    la $a1, aSessionUid # "SESSION_UID="
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    nop
  
```

```

main:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_405F28
    lui $a0, 0x40

loc_405F28:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_405F34
    lui $a0, 0x40

loc_405F34:
    la $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    jalr $t9, aAuthorizedGroup # "AUTHORIZED_GROUP"
    move $a0, $v0 # s
    lw $gp, 0x48+var_30($sp)
    bne $v0, loc_406100
    lui $a0, 0x40

loc_405F28:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_405F34:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_406100:
    la $t9, sess_validate
    addiu $s0, $sp, 0x48+var_28
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, sprintf
    move $a2, $v0 # s
    move $a0, $a0 # s
    jalr $t9, sprintf # "AUTHORIZED_GROUP=%d"
    la $a1, aAuthorizedGroup_0 # "AUTHORIZED_GROUP=%d"
    move $a1, $a0
    la $t9, obj_add_string
    nop
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    move $a0, $a1
    la $t9, obj_add_char
    nop
    jalr $t9, obj_add_char
    li $a1, 0xA
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, obj_add_string
    la $a1, aSessionUid # "SESSION_UID="
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    nop
  
```

```

loc_405F28:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_405F34:
    la $t9, objbin_parse_request
    la $a0, sub_405AC0
    addiu $a0, (sub_405C98 - 0x400000)

loc_406100:
    la $t9, sess_validate
    addiu $s0, $sp, 0x48+var_28
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, sprintf
    move $a2, $v0 # s
    move $a0, $a0 # s
    jalr $t9, sprintf # "AUTHORIZED_GROUP=%d"
    la $a1, aAuthorizedGroup_0 # "AUTHORIZED_GROUP=%d"
    move $a1, $a0
    la $t9, obj_add_string
    nop
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    move $a0, $a1
    la $t9, obj_add_char
    nop
    jalr $t9, obj_add_char
    li $a1, 0xA
    lw $gp, 0x48+var_30($sp)
    lui $a1, 0x42
    la $t9, obj_add_string
    la $a1, aSessionUid # "SESSION_UID="
    jalr $t9, obj_add_string
    move $a0, $a1
    lw $gp, 0x48+var_30($sp)
    nop
  
```