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

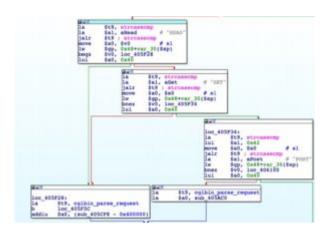
But, the functions sub_405CF8() is executed before sess_validate()

sub_405CF8() is where you get the AUTHORIZED_GROUP value.

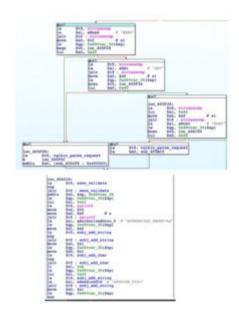
phpogi_main() fund :		
aPost_0:	ascil " POST "40>	# DATA ENERS and 405ACO+4CTs
Bross_01	alien 4	· DRIN AND I HOP TO ME OTHER
ariles	asell " FILES "co>	# DATA EREF: sub 405AC0+B4To
off 4207981	.word los 41274C+2	# DATA XREFT sub 405AC0411470
		# main 425ACD+1F4To
aFiletypes:	.ascii " FILETYPES *+0>	# DATA XNEFT and 405ACO+164To
aGet 0:	aseil "GET_"<0>	# DATA EREF: sub 405CF8+38To
	,alies 4	
Alerveri	.acoli " SERVER "<0>	# DAVA EREFy phycel main+907o
	.aliga 2	
aRequestNethods	.ascii "REQUEST METHOD" «	10
		# DATA XBEF: phpcgl main+F4To
		# diaps main-cmcTo
	.alien 2	
alleads	.ascil "HERO"<0>	# DATA EMEF: phpcgi main+1087a
	.align 7	a contract of the second se
aGet:	.ascii "GET"<0>	# DATA XREF: phpcel main+12870
		# mensioncyl main+70To
aPosts	.ascil "POST" <d></d>	# DATA EREF: physical main+1607cc
		# dlaph main-C9570
	.align 4	
aRtdocsWebIsfoP	.ascii "/htdocs/wsb/info	.php*<0>
		# DATA XREF's phycel main+1A8To
		# dlaps main-C24To +++
	.align 2	
ainfoPhps	.aseli "/info.php"<0>	# DATA EMEF: phpogi main+1P4To
	.align 2	
aFail:	.ascii "FAIL" 40>	# DATA EREF: phpcql main+1F87c
		# diam mais-B30To
	.align 2	
allrrReqTosLong:	.secil "ERR_REQ_TOO_LONG	
		# DATA ENTY: phongl main+1FCTs
	Contraction of the second s	# dlaph main-B2CTo
	.align 4	
aUnsupportedlitt	Laseli "unsupported MTTP	
		# DATA MREY: physici maisilos 405PF47o
	the second s	# diaph main:loc 4071147o
	.align 2	
aAuthorizedGrou	0:.ascii "AUTRORIEED_GRO	
		# DATA XREF: phpcqi main+25CTm
aSessionUid:	.escil "SEESION_UID-"40>	
	alter A	# DATA IRSF: phpergi main+29CTo

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

Proof of Concept



loc_40	\$t9, sess validate
nop	
jalr	St9 ; sess validate
addiu	\$s0, \$sp, 0x48+var 28
lw	\$qp, 0x48+var 30(\$sp)
lui	\$a1, 0x42
1a	St9, sprintf
nove	Sa2, Sv0
move	Sa0, Ss0 # s
jalr	St9 ; sprintf
la	\$al, aAuthorizedGrou_0 # "AUTHORIZED_GROUP=%d"
lw	\$qp, 0x48+var 30(\$sp)
nove	Sal, Ss0
la	\$t9, sobj add string
nop	
jalr	<pre>\$t9 ; sobj_add_string</pre>
move	Sa0, Ss1
lw	\$gp, 0x48+var 30(\$sp)
move	Sa0, Sal
la	\$t9, sobj add char
nop	
jalr	\$t9 ; sobj add char
11	Sal, OxA
lw	Sgp, 0x48+var 30(Ssp)
lui	\$a1, 0x42
la	\$t9, sobj_add_string
1a	\$al, aSessionUid # "SESSION_UID="
jalr	<pre>\$t9 ; sobj_add_string</pre>
nove	\$a0, \$s1
lw	\$gp, 0x48+var_30(\$sp)
nop	The second s



			jair la lw boss lui	Eal, sPost	var_30(\$ep) 56100
41 200_4057281	La \$45, cribin parse La \$45, sub_405AC0		arse_request		
la 515, ogibis_parss_request b log_415F3C addis_5s0, (sub_405CFS - 0x410000)					