Package swiftmailer/swiftmailer 0day GMP RCE

To build exploit for GMP Type Confusion bug we need to find in code:
1) Class that implements Serializable interface
2) Code line executed from __destruct method to rewrite object property
3) Find an object to rewrite props

Package “swiftmailer/swiftmailer” and "pear/net_geoip" were taken for analysis.

```
$ cat composer.json
{
   "require": {
      "swiftmailer/swiftmailer": "5.4.12",
      "pear/net_geoip":"1.0"
   },
   "minimum-stability": "dev"
}
$ composer install
```

1) Search for class with Serializable interface.
File pear/net_geoip/Net/GeoIP/Location.php
class Net_GeoIP_Location implements Serializable

```
120     public function unserialize($serialized)
121     {
122         $this->aData = unserialize($serialized);
123     }
124
```

2) Search for code line to rewrite object property that is reachable from __destruct.

File swiftmailer/lib/classes/Swift/Transport/AbstractSmtpTransport.php

abstract class Swift_Transport_AbstractSmtpTransport implements Swift_Transport

```
492     public function __destruct()
493     {
494         try {
495             $this->stop();
496         } catch (Exception $e) {
497         }
498     }
499 }
```

```
205     public function stop()
206     {
207         if ($this->_started) {
208             if ($evt = $this->_eventDispatcher->createTransportChangeEvent($this)) {
209                 $this->_eventDispatcher->dispatchEvent($evt, 'beforeTransportStopped');
210                 if ($evt->bubbleCancelled()) {
211                     return;
212                 }
213             }
214 
215             try {
216                 $this->executeCommand("QUIT\r\n", array(221));
217             } catch (Swift_TransportException $e) {
218             }
```

Need set some properties in serialized string to get into “write” method of class Swift_CharacterStream_NgCharacterStream.

File swiftmailer/lib/classes/Swift/CharacterStream/NgCharacterStream.php

```
250     public function write($chars)
251     {
252         if (!isset($this->_charReader)) {
253             $this->_charReader = $this->_charReaderFactory->getReaderFor(
254                 $this->_charset);
255             $this->_map = array();
256             $this->_mapType = $this->_charReader->getMapType();
257         }
258         $ignored = '';
259         $this->_datas .= $chars;
260         $this->_charCount += $this->_charReader->getCharPositions(substr($this->
                _datas, $this->_datasSize), $this->_datasSize, $this->_map, $ignored);
```

File swiftmailer/lib/classes/Swift/CharacterReader/GenericFixedWidthReader.php

```
46     public function getCharPositions($string, $startOffset, &$currentMap, &$ignoredChars)
47     {
48         $strlen = strlen($string);
49         // % and / are CPU intensive, so, maybe find a better way
50         $ignored = $strlen % $this->_width;
51         $ignoredChars = $ignored ? substr($string, -$ignored) : '';
52         $currentMap = $this->_width;
53 
54         return ($strlen - $ignored) / $this->_width;
55     }
```

getCharPositions called in line 260 with third argument $this→_map property**.**
In getCharPositions method third parameter $currentMap is passed by reference. And on line 52 it is modified: $currentMap = $this→_width;
This is what we are searching for.
$this→_map is a reference to GMP object, on line 52 it is rewritten with integer zval.

3) Use Composer object with handle = 0x1.