



Experts Warn of Severe Flaws Affecting Milesight Routers and Titan SFTP Servers

Oct 17, 2023 Ravie Lakshmanan Data Security / Network Security

```
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: d(sys.argv[1])
        - Username: admin
        - Password: sv5114871 d(sys.argv[1]) == '-f':
bipin@bipin-VirtualBox:~/ursalink$ python3 ursalink3.py -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 with a list of URLs. (red)
[*] Extracting and decrypting credentials for: https://[REDACTED]:443le.com', '
[+] Unique Credentials:
Example: python3 + sys.argv[0] + '-f urls.txt', 'blue')
Credential 1:
```

A severity flaw impacting industrial cellular routers from **Milesight** may have been actively exploited in real-world attacks, new findings from VulnCheck reveal.

Tracked as [CVE-2023-43261](#) (CVSS score: 7.5), the vulnerability has been described as a case of information disclosure that affects UR5X, UR32L, UR32, UR35, and UR41 routers before version 35.3.0.7 that could enable attackers to access logs such as httpd.log as well as other sensitive credentials.

As a result, this could permit remote and unauthenticated attackers to gain unauthorized access to the web interface, thereby making it possible to configure VPN servers and even drop firewall protections.

"This **vulnerability** becomes even more severe as some routers allow the sending and receiving of SMS messages," security researcher Bipin Jitiya, who discovered the issue, **said** earlier this month. "An attacker could exploit this functionality for fraudulent activities, potentially causing financial harm to the router owner."

Top 2024 SaaS Security Risks

READ THE REPORT

Now, according to VulnCheck's Jacob Baines, there is evidence that the flaw may have been exploited on a small-scale in the wild.



Trending News

- ...

New Grandoreiro Banking Malware Variants Emerge with Advanced Tactics to Evade Detection
- ...

Eliminating AI Deepfake Threats: Is Your Identity Security AI-Proof?
- ...

Permiso State of Identity Security 2024: A Shake-up in Identity Security Is Looming Large
- ...

Notorious Hacker Group TeamTNT Launches New Cloud Attacks for Crypto Mining
- ...

Researchers Uncover OS Downgrade Vulnerability Targeting Microsoft Windows Kernel

"We observed [5.61.39.\]232](#) attempting to log into six systems on October 2, 2023," Baines [said](#). "The affected systems' IP addresses geolocate to France, Lithuania, and Norway. They don't appear to be related, and all use different non-default credentials."

On four of the six machines, the threat actor is said to have successfully authenticated on the first attempt. On the fifth system, the login was successful the second time, and on the sixth, the authentication resulted in failure.

The credentials used to pull off the attack were extracted from the httpd.log, alluding to the weaponization of CVE-2023-43261. There is no evidence of any further malicious actions, although it appears that the unknown actor checked the settings and status pages.

According to VulnCheck, while there are approximately 5,500 internet-exposed Milesight routers, only about 5% are running vulnerable firmware versions, and hence susceptible to the flaw.

"If you have a Milesight Industrial Cellular Router, it's probably wise to assume all the credentials on the system have been compromised and to simply generate new ones, and ensure no interfaces are reachable via the internet," Baines said.


Six Flaws Discovered in Titan MFT and Titan SFTP Servers

The disclosure comes as Rapid7 detailed several security flaws in South River Technologies' Titan MFT and Titan SFTP servers that, if exploited, could allow remote superuser access to affected hosts.

The list of vulnerabilities is as follows -

- [CVE-2023-45685](#) - Authenticated Remote Code Execution via "Zip Slip"
- [CVE-2023-45686](#) - Authenticated Remote Code Execution via WebDAV Path Traversal
- [CVE-2023-45687](#) - Session Fixation on Remote Administration Server
- [CVE-2023-45688](#) - Information Disclosure via Path Traversal on FTP
- [CVE-2023-45689](#) - Information Disclosure via Path Traversal in Admin Interface
- [CVE-2023-45690](#) - Information Leak via World-Readable Database + Logs

"Successful exploitation of several of these issues grants an attacker remote code execution as the root or SYSTEM user," the company [said](#). "However, all issues are post-authentication and require non-default configurations and are therefore unlikely to see wide scale exploitation."

Found this article interesting? Follow us on [Twitter](#)  and [LinkedIn](#) to read more exclusive content we post.

 Tweet

 Share

 Share

 Share

- ...

Researchers Uncover Vulnerabilities in Open-Source AI and ML Models
- ...

A Sherlock Holmes Approach to Cybersecurity: Eliminate the Impossible with Exposure...
- ...

Massive Git Config Breach Exposes 15,000 Credentials; 10,000 Private Repos Cloned
- ...

New LightSpy Spyware Version Targets iPhones with Increased Surveillance Tactics
- ...

Chinese Hackers Use CloudScout Toolset to Steal Session Cookies from Cloud Services
- ...

Microsoft Warns of Chinese Botnet Exploiting Router Flaws for Credential Theft

— Popular Resources

- ...

Check Out This Demo on How to Identify and Patch SaaS Vulnerabilities Before Hackers Do
- ...

Is Your Security Operations Center (SOC) Underperforming? Here's How to Fix It Fast
- ...

Get the 24-Page Guide Every CISO Needs: AI-Driven NDR and Cyber Resilience
- ...

Free Tool Uncovers Weak Passwords and Policies in Your Active Directory

Secure Your Certificates, Fast!

Learn to Automate Certificate Replacement to Avoid Disruptions

Prevent disruptions from certificate revocations with fast, automated solutions for continuity.

Join the Webinar

Make Cybersecurity Memorable!

Learn How to Turn Boring Security Training into Stories They'll Love

Discover how Huntress SAT transforms security training with storytelling, gamification, and real-world examples

Register for Free

— Breaking News

— Cybersecurity Resources

...

Ultimate Guide to Cloud Security

Tackle the unique challenges of cloud security with this expert guide.

...

2024 GigaOm Report: Top SSPM Solutions for Protecting SaaS Environments

Explore GigaOm's 2024 SSPM Radar Report with top vendor insights for securing SaaS data.

...

Permiso Security's 2024 State of Identity Security Report

More than 90% of respondents expressed concern over their team and tooling's ability to detect identity-based attacks. Learn about critical gaps in security programs and what environments pose the most risk to security teams. Download the Report.

...

CISO, Enhance Your Cyber Risk Reporting to the Board

Struggling to convey cybersecurity risks to your board? Our eBook offers actionable insights for CISOs, helping you present accurate, meaningful reports with confidence. Elevate your board presentations—download your guide today.

— Expert Insights / Videos Articles

...

Master Privileged Access Management: Best Practices to Implement

📅 October 14, 2024

Read →

...

Will the Small IoT Device OEM Survive?

📅 October 07, 2024

Read →

...

The Microsoft 365 Backup Game Just Changed: Ransomware Recovery Revolutionized

📅 September 19, 2024

Read →

...

Security Operations for Non-Human Identities

📅 September 28, 2024

Watch →

Get Latest News in Your Inbox

Get the latest news, expert insights, exclusive resources, and strategies from industry leaders – all for free.

Your e-mail address



Connect with us!



925,500 Followers



601,000 Followers



22,700 Subscribers



147,000 Followers



1,890,500 Followers



132,000 Subscribers

Company

- About THN
- Advertise with us
- Contact

Pages

- Webinars
- Deals Store
- Privacy Policy

Deals

- Hacking
- Development
- Android

 RSS Feeds

 Contact Us