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

Oct 17, 2023 Ravie Lakshmanan

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."

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

"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.

— Breaking News

— Cybersecurity Resources

— Expert Insights / Videos Articles

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

RSS Feeds

Contact Us