Una vulnerabilidad grave que afecta a los enrutadores celulares industriales fabricados por Milesight podría haber sido explotada en ataques reales, según descubrimientos recientes de VulnCheck.

Identificada bajo el nombre de CVE-2023-43261 (con una puntuación de CVSS de 7.5), esta vulnerabilidad se describe como un caso de divulgación de información que impacta a los enrutadores modelos UR5X, UR32L, UR32, UR35 y UR41 previos a la versión 35.3.0.7. Esta falla podría permitir a atacantes acceder a registros como httpd.log y a otros datos confidenciales.

Como resultado, esto habilitaría a atacantes remotos y no autenticados a obtener acceso no autorizado a la interfaz web, lo que a su vez les permitiría configurar servidores VPN e incluso desactivar las protecciones del firewall.

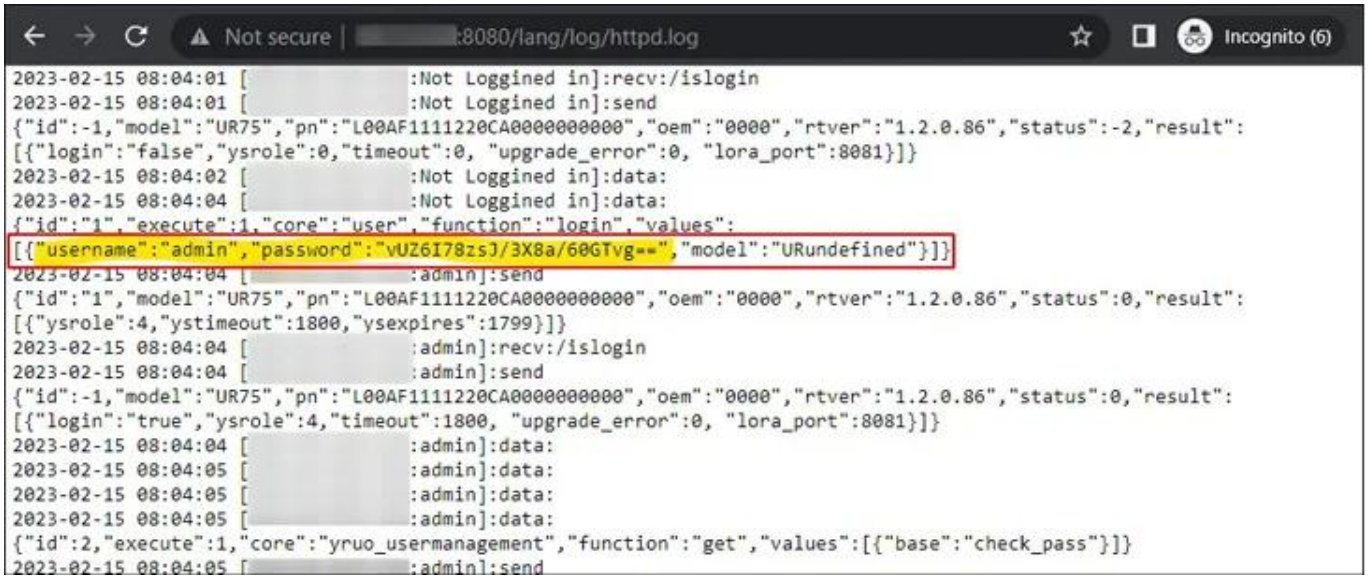
> *«Esta vulnerabilidad se torna aún más crítica debido a que algunos enrutadores permiten el envío y la recepción de mensajes SMS. Un atacante podría aprovechar esta funcionalidad para llevar a cabo actividades fraudulentas, con el potencial de causar daño financiero al propietario del enrutador»,* mencionó el investigador de seguridad Bipin Jitiya, quien descubrió esta vulnerabilidad a principios de este mes.

Ahora, según Jacob Baines de VulnCheck, existen pruebas de que esta falla pudo haber sido utilizada en una pequeña cantidad de ataques en entornos reales.

> *«Observamos que la dirección IP 5.61.39[.]232 intentó iniciar sesión en seis sistemas el 2 de octubre de 2023. Las direcciones IP de los sistemas afectados se ubican en Francia, Lituania y Noruega. No parecen estar relacionados entre sí y todos usan credenciales distintas a las predeterminadas»*, afirmó Baines.

En cuatro de los seis sistemas, se informa que el actor malicioso logró autenticarse con éxito

en el primer intento. En el quinto sistema, el inicio de sesión tuvo éxito en el segundo intento, mientras que en el sexto, la autenticación resultó fallida.



Las credenciales utilizadas para llevar a cabo el ataque fueron extraídas del archivo httpd.log, lo que sugiere la explotación de la CVE-2023-43261. No hay evidencia de acciones maliciosas adicionales, aunque se observa que el actor desconocido revisó la configuración y las páginas de estado.

Según VulnCheck, aunque aproximadamente 5,500 enrutadores Milesight están expuestos en Internet, solo alrededor del 5% de ellos están utilizando versiones de firmware vulnerables y, por lo tanto, son susceptibles a esta falla.

> *«Si posee un Enrutador Celular Industrial de Milesight, es prudente asumir que todas las credenciales del sistema han sido comprometidas y, en consecuencia, debería generar nuevas credenciales. Además, asegúrese de que ninguna interfaz sea accesible desde Internet»,* recomendó Baines.

Se han encontrado seis debilidades en los servidores Titan MFT y Titan SFTP.

Este hallazgo se produce en el contexto de la revelación de Rapid7 de varias vulnerabilidades de seguridad en los servidores Titan MFT y Titan SFTP de South River Technologies. Estas vulnerabilidades, si fueran aprovechadas, podrían permitir el acceso remoto como superusuario a los sistemas afectados.

La lista de vulnerabilidades es la siguiente:

- CVE-2023-45685 – Ejecución remota de código autenticada a través de la vulnerabilidad «Zip Slip».
- CVE-2023-45686 – Ejecución remota de código autenticada a través de la vulnerabilidad de Traversal de Ruta en WebDAV.
- CVE-2023-45687 – Fijación de sesiones en el Servidor de Administración Remota.
- CVE-2023-45688 – Divulgación de información mediante la Traversal de Ruta en FTP.
- CVE-2023-45689 – Divulgación de información a través de la Traversal de Ruta en la Interfaz de Administración.
- CVE-2023-45690 – Fuga de información a través de una Base de Datos y Registros de Lectura Mundial.

> *«La explotación exitosa de varias de estas vulnerabilidades concede a un atacante la ejecución de código remoto con privilegios de root o SYSTEM. No obstante, todas estas vulnerabilidades requieren autenticación previa y configuraciones no predeterminadas, por lo que es poco probable que se produzca una explotación generalizada»,* afirmó la empresa.