Se ha revelado una vulnerabilidad de seguridad de gravedad elevada en la función de análisis de URL de Python, la cual podría ser aprovechada para eludir métodos de filtrado de dominio o protocolo implementados con una lista de bloqueo, lo que en última instancia resultaría en la posibilidad de leer archivos arbitrarios y ejecutar comandos de manera no autorizada.

El Centro de Coordinación de CERT (CERT/CC) comunicó en un aviso publicado el viernes que *«la función 'urlparse' presenta un problema en su análisis cuando la URL completa comienza con caracteres en blanco».* Esto afecta tanto al análisis del nombre de dominio como al esquema, y puede llevar a la ineficacia de cualquier método de bloqueo utilizado.

La vulnerabilidad ha sido identificada con el código CVE-2023-24329 y se le ha asignado un puntaje CVSS de 7.5. El investigador de seguridad Yebo Cao ha sido reconocido por descubrir y notificar el problema en agosto de 2022. Las versiones afectadas han sido corregidas en las siguientes iteraciones:

- >= 3.12
- 3.11.x >= 3.11.4
- 3.10.x >= 3.10.12
- 3.9.x >= 3.9.17
- 3.8.x >= 3.8.17
- 3.7.x >= 3.7.17

La biblioteca `urllib.parse` es ampliamente empleada para la función de análisis que descompone las URL en sus elementos constituyentes, o en su lugar, combina los componentes para formar una cadena URL completa.

La vulnerabilidad CVE-2023-24329 surge debido a la carencia de validación de los datos de entrada, lo que conduce a una situación donde es posible sortear los métodos de bloqueo al suministrar una URL que comienza con caracteres en blanco (por ejemplo, «https://youtube[.]com»).

> *«Aunque el uso de listas de bloqueo se considera una opción menos preferible, todavía existen numerosos escenarios donde son necesarias. Esta vulnerabilidad permitiría a un atacante evadir las protecciones establecidas por el desarrollador para el esquema y el host. Se espera que esta vulnerabilidad contribuya a la explotación de vulnerabilidades SSRF (Falsificación de solicitud entre sitios) y RCE (Ejecución remota de comandos) en una amplia variedad de situaciones»*, comentó Cao.