Amazon solucionó un problema de seguridad de alta gravedad en su aplicación Ring para Android en mayo, que podría haber permitido que una aplicación no autorizada instalada en el dispositivo de un usuario accediera a información confidencial y grabaciones de cámaras.

La aplicación de Ring para Android tiene más de 10 millones de descargas y permite a los usuarios monitorear transmisiones de video desde dispositivos domésticos inteligentes como timbres de video, cámaras de seguridad y sistemas de alarma. Amazon adquirió el fabricante de timbres por alrededor de mil millones de dólares en 2018.

La compañía de seguridad de aplicaciones Checkmarx explicó que identificó una falla de secuencias de comandos en sitios cruzados (XSS) que, según dijo, podría convertirse en un arma como parte de una cadena de ataque para engañar a las víctimas para que instalen una aplicación maliciosa.

Después, la aplicación se puede usar para obtener el token de autorización del usuario, que luego puede aprovecharse para extraer la cookie de sesión enviando esta información junto con la identificación del hardware del dispositivo, que también está codificada en el token, al punto final *«ring[.]com/movil/autorizar»*.

Armado con esta cookie, el atacante puede iniciar sesión en la cuenta de la víctima sin tener que conocer su contraseña y acceder a todos los datos personales asociados con la cuenta, incluyendo el nombre completo, dirección de correo electrónico, número de teléfono y la información de geolocalización, así como las grabaciones del dispositivo.

Esto se puede lograr al consultar los siguientes puntos:

- account.ring[.]com/account/control-center: Obtener la información personal del usuario y el ID del dispositivo
- account.ring[.]com/api/cgw/evm/v2/history/devices/{{DEVICE_ID}}: Accede a los datos y grabaciones del dispositivo Ring

Checkmarx dijo que informó el problema a Amazon el 1 de mayo de 2022, después de lo cual se puso a disposición una solución el 27 de mayo en la versión 3.51.0. No existe evidencia de que el problema haya sido explotado en ataques del mundo real, con Amazon caracterizando el exploit como *«extremadamente difícil»* y enfatizando que no se expuso información del cliente.