Se revelaron cuatro vulnerabilidades de alta gravedad en un marco utilizado por aplicaciones del sistema Android preinstaladas con millones de descargas.

Los problemas, ya resueltos por su desarrollador israelí MCE Systems, podrían haber permitido potencialmente que los actores de amenazas realicen ataques remotos y locales o que se abuse de ellos como vectores para obtener información confidencial aprovechando sus amplios privilegios de sistema.

> *«Como sucede con muchas de las aplicaciones preinstaladas o predeterminadas que vienen con la mayoría de los dispositivos Android en estos días, algunas de las aplicaciones afectadas no se pueden desinstalar o deshabilitar por completo sin obtener acceso de root al dispositivo»*, dijo el equipo de investigación de Microsoft 365 Defender en un informe.

A las vulnerabilidades, que van desde la inyección de comandos hasta la escalada de privilegios locales, se les asignó los identificadores CVE-2021-42598, CVE-2021-42599, CVE-2021-42600 y CVE-2021-42601, con puntajes CVSS entre 7.0 y 8.9.

Microsoft no reveló la lista completa de aplicaciones que utilizan el nuevo marco vulnerable en cuestión, que está diseñado para ofrecer mecanismos de autodiagnóstico para identificar y solucionar problemas que afectan a un dispositivo Android.

Esto también significó que el marco tenía amplios permisos de acceso, incluyendo audio, cámara, energía, ubicación, datos de sensores y almacenamiento, para llevar a cabo sus funciones. Junto con los problemas identificados en el servicio, Microsoft dijo que podría

permitir que un atacante implante puertas traseras persistentes y tome el control.

Algunas de las aplicaciones afectadas son de grandes proveedores internacionales de servicios móviles, como Telus, AT&T, Rogers, Freedom Mobile y Bell Canada.

- Comprobación de dispositivos de Mobile Klinik (com.telus.checkup)
- Ayuda del dispositivo (com.att.dh)
- MyRogers (com.fivemobile.myaccount)
- Freedom Device Care (com.freedom.mlp.uat)
- Transferencia de contenido del dispositivo (com.ca.bell.contenttransfer)

Además, Microsoft recomienda a los usuarios que busquen el paquete de la aplicación *«com.mce.mceiotraceagent»*, una aplicación que puede haber sido instalada por talleres de reparación de teléfonos móviles, y que la eliminen de los teléfonos, si la encuentran.

Las aplicaciones susceptibles, aunque preinstaladas por los proveedores de telefonía, también están disponibles en Google Play Store y se dice que han superado los controles de seguridad automáticos de la tienda de aplicaciones sin generar ninguna señal de alerta porque el proceso no fue diseñado para detectar estos problemas, algo que ya se había corregido.