Múltiples vulnerabilidades descubiertas en los parlantes inalámbricos Sonos One, podrían explotarse potencialmente para lograr la divulgación de información y la ejecución remota de código, dijo Zero Day Initiative (ZDI) en un informe de la semana pasada.

Las vulnerabilidades fueron demostradas por tres equipos distintos de Qrious Secure, STAR Labs y DEVCORE en el concurso de hacking Pwn20wn realizado en Toronto a fines del año pasado, lo que les significó $105,000 dólares en recompensas.

Las cuatro vulnerabilidades que afectan a Sonos One Speaker 70.3-35220 se detallan a continuación:

- CVE-2023-27352 y CVE-2023-27355 (puntaje CVSS: 8.8): Vulnerabilidades no autenticadas que permiten a los atacantes adyacentes a la red ejecutar código arbitrario en las instalaciones afectadas.
- CVE-2023-27353 y CVE-2023-27354 (puntaje CVSS: 6.5): Vulnerabilidades no autenticadas que permiten a los atacantes adyacentes a la red revelar información confidencial sobre las instalaciones afectadas.

Mientras que CVE-2023-27352 proviene del procesamiento de comandos de consulta de directorio SMB, CVE-2023-27355 existe dentro del analizador MPEG-TS.

La explotación exitosa de las dos vulnerabilidades podría permitir que un atacante ejecute código arbitrario en el contexto del usuario raíz.

Ambas vulnerabilidades de divulgación de información se pueden combinar por separado con otras fallas en los sistemas para lograr la ejecución de código con privilegios elevados.

Después de la divulgación responsable el 20 de diciembre de 2022, Sonos solucionó las vulnerabilidades como parte de las versiones 15.1 y 11.7.1 del software Sonos S2 y S1, respectivamente. Se recomienda a los usuarios que apliquen los últimos parches para mitigar potenciales riesgos.