Recuperar acceso root mediante cambio de contraseña

Reiniciando el sistema

- Reiniciar el sistema y presione cualquier tecla para detener el proceso de inicio. Presione “e” para editar los parámetros de la línea de comandos del kernel.
- Adicionar el parámetro “init=/bin/bash“ e iniciar el sistema (F10)
- Para montar el sistema de archivos raíz en “modo lectura-escritura”.
- Cambiar el password con el comando passwd
- Reiniciar el sistema y ingresar con el nuevo password

Sin reiniciar el sistema

La unica opcion para este escenario es la ejecución romota de código (RCE) mediante la explotación de alguna vulnerabilidad para cambiar password del usuario root. Las vulnerabilidades identificadas para Debian 9 son:

- CVE-2019-11815 Dificil de explotar y existe una gran probabilidad de causar una denegacion de servicio. No existe exploit público
- CVE-2020-15862 No existe exploit público

Fuente: https://security-tracker.debian.org/tracker/CVE-2019-11815

Revision #2
Created 10 marzo 2023 11:49:34 by Franz Rojas
Updated 3 abril 2025 12:30:23 by Vladimir Urquiola