HP publicó una alerta de seguridad para informar sobre tres vulnerabilidades críticas en su producto HP Device Manager, que de explotarse, podría comprometer los sistemas afectados.

Según el reporte, la explotación de las vulnerabilidades podría permitir a los hackers obtener privilegios SYSTEM remotamente en dispositivos que ejecutan versiones vulnerables de HP Device Manager. También puede permitir realizar ataques de diccionario, acceso no autorizado a recursos restringidos y escaladas de privilegios.

Las vulnerabilidades en cuestión son:

- CVE-2020-6925: Las cuentas que se administran localmente se exponen a ataques de diccionario debido a una implementación débil de cifrado. La falla afecta a todas las versiones de HP Device Manager.
- CVE-2020-6926: Es una falla de invocación de método remoto en todas las versiones de HP Device Manager, que permite a los hackers obtener acceso no autorizado a los recursos del sistema.
- CVE-2020-6927: Esta vulnerabilidad puede permitir a los hackers obtener privilegios SYSTEM a través de un usuario de base de datos de backdoor en la base de datos PostgreSQL.

Esta última vulnerabilidad no afecta a los clientes de HP que utilizan una base de datos externa, como Microsoft SQL Server, y no han instalado el servicio Postgres integrado.

Para la vulnerabilidad CVE-2020-6927, es posible mitigar el riesgo al descargar la versión 5.0.4 de HP Device Manager. En cuando a las otras vulnerabilidad, aún no existen actualizaciones, pero es posible protegerse con las siguientes recomendaciones:

- Limitar el acceso entrante a los puertos 1099 y 40002 del Administrador de Dispositivos a IPs configables, o únicamente localhost.
- Eliminar la cuenta dm_postgres de la base de datos Postgres.
- Actualizar la contraseña de la cuenta dm_postgres dentro de HP Device Manager Configuration.