BOLETÍN DE ALERTA

Boletín Nro.: 2022-13

Fecha de publicación: 02/03/2022

Tema: Vulnerabilidades críticas en Fabric OS

Software afectado:

- Brocade Fabric OS versiones anteriores a 8.2.1c y 8.1.2h

Descripción:

Se han publicado parches de seguridad para subsanar dos vulnerabilidades críticas identificadas como CVE-2021-27797 y CVE-2021-27796 en la guía de administración de Brocade Fabric OS, que permitirían a un atacante obtener acceso al equipo de la víctima.

- CVE-2021-27797 de severidad crítica, con una puntuación de 9.8 asignada. Esta se debe a en la documentación proveída por el fabricante se incluyeron credenciales por defecto débiles incrustadas que debían cambiarse, sin embargo, muchos administradores omitieron el mensaje. Un atacante podría explotar esta vulnerabilidad para conectarse a los sistemas afectados mediante SSH *(SecureShell)*, obtener acceso a un entorno de *shell* restringido (*rbash*) y la capacidad de leer archivos con permisos privilegiados de los usuarios “user” y “factory”.

- CVE-2021-27796, de severidad crítica, sin puntuación asignada aún. Esta vulnerabilidad de lectura de archivos privilegiados permitiría a un atacante autenticado obtener acceso al contenido de archivos arbitrarios. Los binarios utilizados incluyen *date*, *grep* y otros más para el usuario ”factory”.

Impacto:

La explotación de estas vulnerabilidades combinadas permitiría a un atacante el acceso al dispositivo vulnerable y la lectura de cualquier archivo con privilegios de los usuarios “user” y “factory”.

Detección:

Verificar si el equipo posee alguna de las siguientes versiones afectadas del software:

- Brocade Fabric OS en sus versiones 8.2.x anteriores a 8.2.1c, 8.1.x anteriores a 8.1.2h, 8.0.x y 7.x (sin soporte actualmente).

Solución:

La aplicación del cambio de contraseña obligatorio fue efectiva en las versiones de Brocade Fabric OS v.9.0.0, v8.2.1c, v8.1.2h y versiones superiores.

Recomendamos instalar las actualizaciones de seguridad correspondientes provistas por Brocade Fabric OS, como se indica en los siguientes enlaces:

Brocade Fabric OS versiones 8.0.x:

- https://docs.broadcom.com/doc/FOS-8X-CM-OT

Brocade Fabric OS v8.2.x

- https://docs.broadcom.com/doc/FOS-821-SW-Upgrade-UG

Brocade Fabric OS v.9.0.0:

- https://docs.broadcom.com/doc/FOS-90x-UPG-UG

Información adicional:

- https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2021-1722
- https://blog.blacklanternsecurity.com/p/privileged-read-and-weak-default?utm_source=url
- https://nvd.nist.gov/vuln/detail/CVE-2021-27797
- https://nvd.nist.gov/vuln/detail/CVE-2021-27796
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27797