Se han revelado múltiples vulnerabilidades de seguridad en la aplicación de gestión de redes de área de almacenamiento (SAN) Brocade SANnav que podrían ser explotadas para comprometer dispositivos susceptibles.

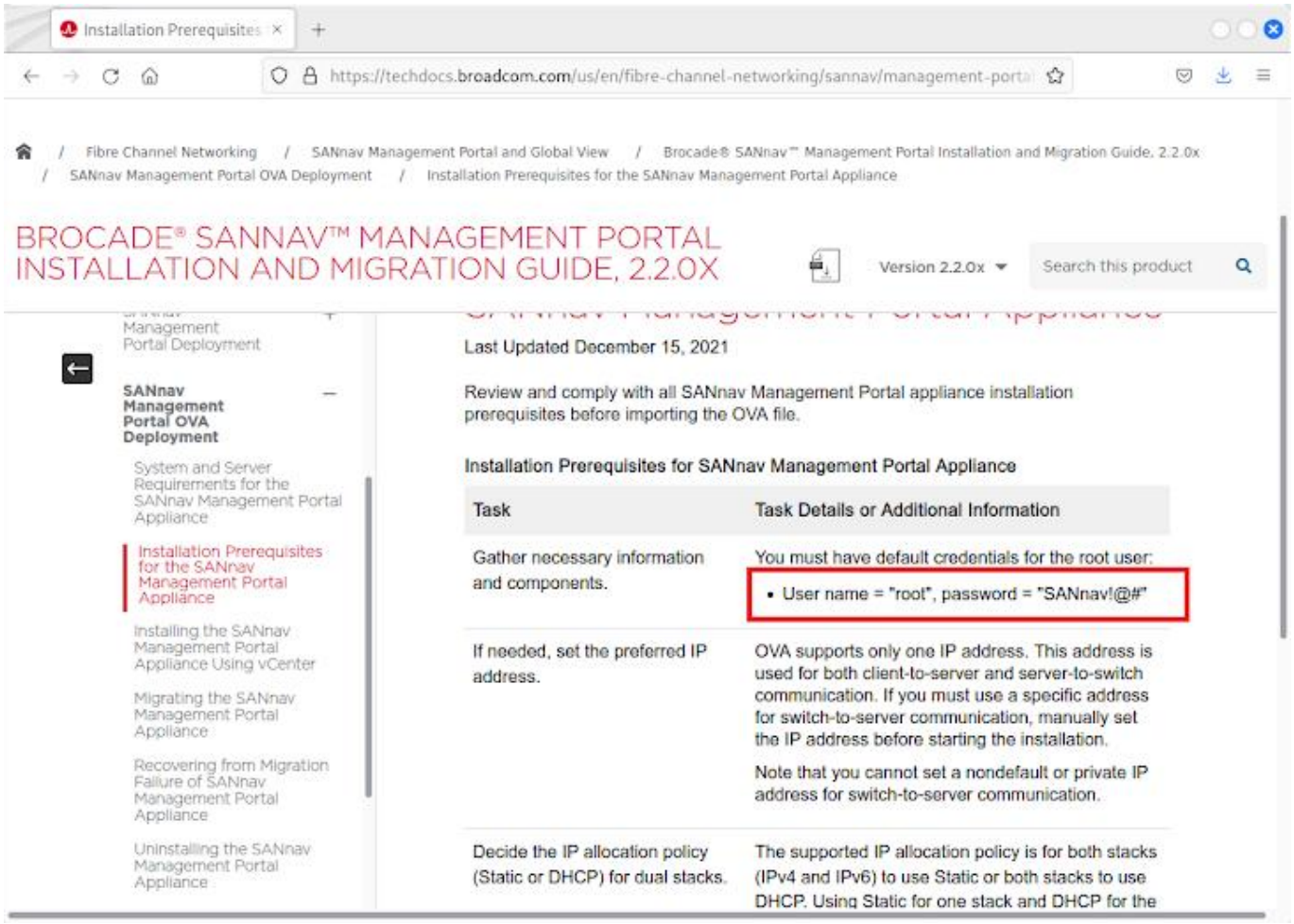
Las 18 debilidades afectan a todas las versiones hasta e incluyendo la 2.3.0, según el investigador de seguridad independiente Pierre Barre, quien las identificó y notificó.

Los problemas abarcan desde configuraciones incorrectas de firewall, acceso root inseguro y fallos de configuración de Docker hasta la ausencia de autenticación y cifrado, lo que posibilita que un atacante intercepte credenciales, modifique archivos arbitrariamente y acceda completamente al dispositivo.

Algunas de las vulnerabilidades más graves se detallan a continuación:

- CVE-2024-2859 (puntuación CVSS: 8.8) – Una falla que podría permitir a un atacante remoto y no autenticado iniciar sesión en un dispositivo afectado utilizando la cuenta root y ejecutar comandos arbitrarios.
- CVE-2024-29960 (puntuación CVSS: 7.5) – El empleo de claves SSH predefinidas en la imagen OVA, lo que podría ser aprovechado por un atacante para descifrar el tráfico SSH hacia el dispositivo SANnav y comprometerlo.
- CVE-2024-29961 (puntuación CVSS: 8.2) – Una debilidad que posibilita a un atacante remoto y no autenticado realizar un ataque de cadena de suministro al aprovechar que el servicio SANnav envía comandos de ping a intervalos periódicos a los dominios gridgain[.]com e ignite.apache[.]org para buscar actualizaciones.
- CVE-2024-29963 (puntuación CVSS: 8.6) – El uso de claves Docker predefinidas en la imagen OVA de SANnav para conectarse a registros remotos mediante TLS, permitiendo a un atacante realizar un ataque de intermediario en el tráfico.
- CVE-2024-29966 (puntuación CVSS: 7.5) – La existencia de credenciales predefinidas para usuarios root en documentación de acceso público que podría permitir a un atacante no autenticado acceso total al dispositivo Brocade SANnav.

Tras una divulgación responsable realizada dos veces en agosto de 2022 y mayo de 2023, las

debilidades han sido abordadas en la versión 2.3.1 de SANnav lanzada en diciembre de 2023. Broadcom, la empresa matriz de Brocade que también posee Symantec y VMware, publicó advertencias sobre las debilidades a principios de este mes.

Hewlett Packard Enterprise también ha lanzado parches para un subconjunto de estas vulnerabilidades en las versiones 2.3.0a y 2.3.1 del Portal de Gestión SANnav de HPE a partir del 18 de abril de 2024.