مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Brocade SANnav SAN Management Application

Tracking #:432315803

Date:30-04-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Multiple vulnerabilities in the Brocade SANnav storage area network (SAN) management application that could be exploited by an attacker to compromise SANnav appliances, potentially leading to unauthorized access, data breaches, and complete device takeover.

TECHNICAL DETAILS:

Vulnerabilities Details:

- CVE-2024-4159 - Incorrect firewall rules
- non-assigned CVE vulnerability - Lack of encryption for management protocol (HTTP)
- CVE-2024-4161 - Syslog traffic sent in clear-text
- CVE-2024-29966 - Insecure root access
- non-assigned CVE vulnerability - Insecure sannav access
- CVE-2024-2859 - Insecure SSH configuration
- CVE-2024-29961 - Suspicious network traffic (ignite.apache.org)
- non-assigned CVE vulnerability - Lack of authentication in Postgres
- CVE-2024-29967 - Insecure Postgres Docker instance
- CVE-2024-29967 - Insecure Docker instances
- CVE-2024-29964 - Insecure Docker architecture and configuration
- CVE-2024-29965 - Insecure Backup process
- CVE-2024-4159 - Inconsistency in firewall rules
- CVE-2024-29962 - Insecure file permissions
- CVE-2024-4173 - Kafka reachable on the WAN interface and Lack of authentication
- CVE-2024-29960 - Hardcoded SSH Keys
- CVE-2024-29961 - Suspicious network traffic (www.gridgain.com)
- CVE-2024-29963 - Hardcoded Docker Keys

Affected Versions:
SANnav versions up to and including 2.3.0

Fixed Versions:
SANnav version 2.3.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://pierrekim.github.io/blog/2024-04-24-brocade-sannav-18-vulnerabilities.html