CYBER ADVISORY

TLP:CLEAR
26 April 2024

Multiple Brocade SANnav Vulnerabilities

Broadcom | Brocade | SANnav Management | High Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple high vulnerabilities within Broadcom Brocade product.[1] The vulnerabilities affect Brocade SANnav storage area network (SAN) management application up to and including versions 2.3.0.[2] Exploitation of selected vulnerabilities may allow an attacker to send malicious data and to intercept credentials sent in clear-text, potentially compromising the entire Fibre Channel infrastructure.[3]

CVE Identifier	Vulnerability Description
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

Table 1: Brocade SANnav Vulnerability Description

The Cal-CSIC recommends applying Brocade SANnav updates as soon as possible.

For further information on applying Brocade SANnav updates, please refer to Broadcom Support and Services.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] The Hacker News; "Severe Flaws Disclosed in Brocade SANnav SAN Management Software;" https://thehackernews.com/2024/04/severe-flaws-disclosed-in-brocade.html; accessed 26 April 2024

[2] Security Week; "Vulnerabilities Expose Brocade SAN Appliances, Switches to Hacking;" https://www.securityweek.com/vulnerabilities-expose-brocade-san-appliances-switches-to-hacking/; accessed 26 April 2024

[3] IT Security Research by Pierre; "18 vulnerabilities in Brocade SANnav;" https://pierrekim.github.io/blog/2024-04-24-brocade-sannav-18-vulnerabilities.html; accessed 26 April 2024