

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
 - [Cloud Security](#)
 - [Identity & Access](#)
 - [Data Protection](#)
 - [Network Security](#)
 - [Application Security](#)
- ▼ [Security Strategy](#)
 - [Risk Management](#)
 - [Security Architecture](#)
 - [Disaster Recovery](#)
 - [Training & Certification](#)
 - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Vulnerabilities](#)



Brocade Vulnerabilities Could Impact Storage Solutions of Several Major Companies

By [Eduard Kovacs](#) on June 30, 2022

Share

Tweet

推荐 0



Broadcom revealed recently that some of the software provided by its storage networking subsidiary Brocade is affected by several vulnerabilities, and it seems possible that the flaws could impact the products of several major companies.

According to Broadcom, the Brocade SANnav storage area network (SAN) management application is affected by nine vulnerabilities. Patches have been made available for these security holes.

Six of them impact third-party components such as OpenSSL, Oracle Java and NGINX, and they have been rated “medium severity” or “low severity”. Exploitation of these flaws can allow an attacker — in many cases unauthenticated attacker — to manipulate data, decrypt data, and cause a denial of service (DoS) condition.

The remaining three vulnerabilities are specific to Brocade SANnav and they have been assigned a “high” severity and risk impact rating. They can allow an attacker to obtain switch and server passwords from log files, and intercept potentially sensitive information due to static key ciphers.

The security bugs ([CVE-2022-28167](#), [CVE-2022-28168](#) and [CVE-2022-28166](#)) were discovered internally and there is no evidence of exploitation in the wild.

However, the storage solutions of several companies that work with Brocade could be affected by these vulnerabilities.

In an advisory published this week, [HPE informed customers](#) that its B-Series SANnav Management Portal is affected by the flaws and advised them to install the latest updates.

“The vulnerabilities could be locally and remotely exploited to disclose sensitive information, perform unauthorized access and modification of data and cause partial Denial of Service,” HPE said.

NetApp, another Brocade partner, has published individual [advisories](#) for the Brocade SANnav-specific vulnerabilities. NetApp’s own products do not appear to be affected.

Brocade also has partnerships with several other tech giants for their storage solutions, including Dell, Fujitsu, Huawei, IBM, and Lenovo.

At the time of writing, none of the other [Brocade OEM partners](#) appear to have published advisories for the SANnav vulnerabilities so it’s unclear if their products are also impacted. In the past, at least some of them did publish advisories to notify their customers about SANnav flaws.

SecurityWeek has reached out to Broadcom for clarifications, but the company has yet to respond.

Related: [Storage Devices of Major Vendors Impacted by Encryption Software Flaws](#)

Related: [Zero-Day Vulnerability Exploited in Recent Attacks on WD Storage Devices](#)

Related: [Old Vulnerability Exploited to Hack, Wipe WD Storage Devices](#)

[Share](#)[Tweet](#)[推荐 0](#)[RSS](#)

Eduard Kovacs ([@EduardKovacs](#)) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia’s security news reporter. Eduard holds a bachelor’s degree in industrial informatics and a master’s degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs:

[Brocade Vulnerabilities Could Impact Storage Solutions of Several Major Companies](#)

[Canadian NetWalker Ransomware Affiliate Pleads Guilty in US](#)

[MITRE Publishes 2022 List of 25 Most Dangerous Vulnerabilities](#)

[CISA Says 'PwnKit' Linux Vulnerability Exploited in Attacks](#)

[New Database Catalogs Cloud Vulnerabilities, Security Issues](#)

[2022 ICS Cyber Security Conference | USA \[Hybrid: Oct. 24-27\]](#)

sponsored links

[2022 CISO Forum: September 13-14 - A Virtual Event](#)

[2022 Singapore/APAC ICS Cyber Security Conference](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

Tags:

[NEWS & INDUSTRY](#) [Vulnerabilities](#)