



# CVE-2021-32522

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

|                        |  |
|------------------------|--|
| <b>CVE</b>             | CVE-2021-32522   |
| <b>State</b>           | PUBLIC   |
| <b>Assigner</b>        | cve@cert.org.tw  |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback   |
| <b>Published</b>       | 2021-07-07 14:15:00 UTC  |
| <b>Updated</b>         | 2021-09-20 12:35:00 UTC  |
| <b>Description</b>     | Improper restriction of excessive authentication attempts vulnerability in QSAN Storage Manager, XEVO, SANOS allows re |

## Risk And Classification

**Problem Types:** CWE-307

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor               | Product                         | Version | Update | Edition | Language |
|-------------|----------------------|---------------------------------|---------|--------|---------|----------|
| Application | <a href="#">Qsan</a> | <a href="#">Sanos</a>           | All     | All    | All     | All      |
| Application | <a href="#">Qsan</a> | <a href="#">Storage Manager</a> | All     | All    | All     | All      |
| Application | <a href="#">Qsan</a> | <a href="#">Xevo</a>            | All     | All    | All     | All      |

## References

### Reference

- TWCERT/CC台灣電腦網路危機處理暨協調中心-QSAN Storage Manager, XEVO, SANOS - Improper Restriction of Excessive Authentication A
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**