



# CVE-2019-12393

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

## Summary

<b>CVE</b>	CVE-2019-12393
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2019-12-02 17:15:00 UTC
<b>Updated</b>	2019-12-12 17:56:00 UTC
<b>Description</b>	Anviz access control devices are vulnerable to replay attacks which could allow attackers to intercept and replay open door

## Risk And Classification

**Problem Types:** CWE-294

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Anviz	Management System	-	All	All	All
Application	Anviz	Management System	-	All	All	All

## References

### Reference

- Anviz Pwn! How broken devices could be? (CVE-2019-12393/CVE-2019-12391/CVE-2019-12392/CVE-2019-12390/CVE-2019-12389/CVE-2019-12388)
- 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.

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](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)