# CVE-2021-32455

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-32455 |
| **State** | PUBLIC |
| **Assigner** | cve-coordination@incibe.es |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-05-17 17:15:00 UTC |
| **Updated** | 2021-05-24 16:41:00 UTC |
| **Description** | SITEL CAP/PRX firmware version 5.2.01, allows an attacker with access to the device´s network to cause a denial of servic |

## Risk And Classification

**Problem Types:** CWE-400

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Sitel-sa | Cap/prx | - | All | All | All |
| Operating System | Sitel-sa | Cap/prx Firmware | 5.2.01 | All | All | All |

## References

| Reference | Source | Link | Tags |
|---|---|---|---|
| SITEL CAP/PRX vulnerable to a denial of service attack \| INCIBE-CERT | CONFIRM | www.incibe-cert.es | |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | canonical, analysis |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** Industrial Cybersecurity team of S21sec, special mention to Aarón Flecha Menéndez and Luis Martín Liras, as an independent researcher.

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