



CVE-2021-32454

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

Summary

CVE	CVE-2021-32454
State	PUBLIC
Assigner	cve-coordination@incibe.es
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-05-17 18:15:00 UTC
Updated	2021-05-25 16:44:00 UTC
Description	SITEL CAP/PRX firmware version 5.2.01 makes use of a hardcoded password. An attacker with access to the device could

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
SITEL CAP/PRX hardcoded credentials 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.

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report