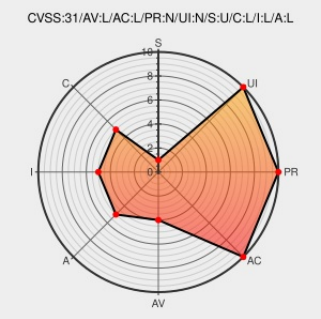
CVE-2017-20040

Published on: Not Yet Published

Last Modified on: 06/17/2022 05:47:00 PM UTC

CVE-2017-20040

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Access Control from Sicunet contain the following vulnerability:

A vulnerability was found in SICUNET Access Controller 0.32-05z. It has been declared as problematic. This vulnerability affects unknown code of the component Password Storage. The manipulation leads to weak encryption. Attacking locally is a requirement.

CVE-2017-20040 has been assigned by cna@vuldb.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **SICUNET** - **Access Controller** version **0.32-05z**

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Full Disclosure: SICUNET Physical Access Controller - Multiple Vulnerabilities	seclists.org, text/html	MISC seclists.org/fulldisclosure/2017/Mar/25

CVE-2017-20040 | SICUNET Access Controller Password Storage cleartext storage

vuldb.com text/html

MISC vuldb.com/?id.98908

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sicunet	Access Control	0.32-05z	All	All	All

cpe:2.3:a:sicunet:access_control:0.32-05z:*:*:*:*:*:*:*

Discovery Credit

Andrew Griffiths

← Previous ID

Next ID→