



CVE-2021-32033

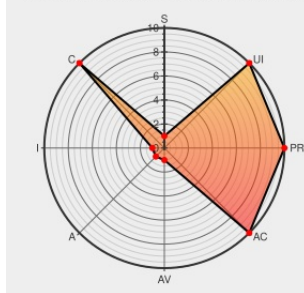
Published on: 06/16/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-32033

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N



Certain versions of [Slim Nfc 70](#) from [Protectimus](#) contain the following vulnerability:

Protectimus SLIM NFC 70 10.01 devices allow a Time Traveler attack in which attackers can predict TOTP passwords in certain situations. The time value used by the device can be set independently from the used seed value for generating time-based one-time passwords, without authentication. Thus, an attacker with short-time physical

access to a device can set the internal real-time clock (RTC) to the future, generate one-time passwords, and reset the clock to the current time. This allows the generation of valid future time-based one-time passwords without having further access to the hardware token.

CVE-2021-32033 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.6 - MEDIUM**

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

CVSS2 Score: **1.9 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
-------------	------	------

www.syss.de
[text/plain](#)

 MISC
www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-007.txt

Protectimus SLIM NFC Time Manipulation ≈ Packet Storm

packetstormsecurity.com
[text/html](#)

 MISC packetstormsecurity.com/files/163223/Protectimus-SLIM-NFC-Time-Manipulation.html

Full Disclosure: [SYSS-2021-007]: Protectimus SLIM NFC - External Control of System or Configuration Setting (CWE-15) (CVE-2021-32033)

seclists.org
[text/html](#)

 FULLDISC 20210618 [SYSS-2021-007]: Protectimus SLIM NFC - External Control of System or Configuration Setting (CWE-15) (CVE-2021-32033)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Protectimus	Slim Nfc 70	-	All	All	All
Operating System	Protectimus	Slim Nfc 70 Firmware	10.01	All	All	All

cpe:2.3:h:protectimus:slim_nfc_70:-:~::~:~::~:~::~:~::~:~::~:

cpe:2.3:o:protectimus:slim_nfc_70_firmware:10.01:~::~:~::~:~::~:~::~:~::~:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @matthiasdeeg	You can find the corresponding security advisory SYSS-2021-007 (CVE-2021-32033) describing this security vulnerabil... twitter.com/i/web/status/1...	2021-06-16 07:23:53
 @CVEreport	CVE-2021-32033 : Protectimus SLIM NFC 70 10.01 devices allow a Time Traveler attack in which attackers can predict... twitter.com/i/web/status/1...	2021-06-16 12:08:50
 /r/netcve	CVE-2021-32033	2021-06-16 12:41:24

← Previous ID

Next ID →

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](#)