Protectimus SLIM NFC Time Manipulation

Authored by Matthias Deeg | Site syss.de

Posted Jun 18, 2021

When analyzing the Protectimus SLIM TOTP hardware token, Matthias Deeg found out that the time used by the Protectimus SLIM TOTP hardware token can be set independently from the used seed value for generating time-based one-time passwords without requiring any authentication.

tags | advisory
advisories | CVE-2021-32033
SHA-256 | 18da959eb49ff3d5b8d29ab92f7247fff8490774b451cce50831a03dc291d6c0 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
Advisory ID: SYSS-2021-007
Product: Protectimus SLIM NFC
Manufacturer: Protectimus
Affected Version(s): Hardware Scheme 70 / Software Version 10.01
Tested Version(s): Hardware Scheme 70 / Software Version 10.01
Vulnerability Type: External Control of System or Configuration Setting
(CWE-15)
                    "Time Traveler Attack"
Risk Level: Medium
Solution Status: Open
Manufacturer Notification: 2021-02-04
Solution Date: -
Public Disclosure: 2021-06-16
CVE Reference: CVE-2021-32033
Author of Advisory: Matthias Deeg (SySS GmbH)

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Overview:

Protectimus SLIM NFC is a reprogrammable time-based one-time password
(TOTP) hardware token.

The manufacturer describes the product as follows (see [1]):

"
Protectimus SLIM mini is a new generation of reprogrammable TOTP
hardware tokens. They can be used in 2FA systems based on OATH
standards, and easily reflashed using an application installed on your
NFC-capable Android smartphone. It allows the user to determine the
OTP's expires (30 or 60 seconds), and also set up a secret key.
"

Due to a design error, the time (internal real-time clock) of the
Protectimus SLIM TOTP hardware token can be set independently from the
used seed (secret key) for generating one-time passwords without any
required authentication.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Vulnerability Details:

When analyzing the Protectimus SLIM TOTP hardware token, Matthias Deeg
found out that the time used by the Protectimus SLIM TOTP hardware token
can be set independently from the used seed value for generating
time-based one-time passwords without requiring any authentication.

Thus, an attacker with short-time physical access to a Protectimus SLIM
token 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 for generating valid future time-based one-time passwords
without having further access to the hardware token.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Proof of Concept (PoC):

For demonstrating the time traveler attack exploiting the described
security vulnerability, Matthias Deeg developed a Lua script for the
Proxmark3 [2].

The following output exemplarily shows a successful attack for
generating a valid future one-time password for an attacker-chosen point
in time against a vulnerable Protectimus SLIM TOTP hardware token:

[usb] pm3 --> script run hf_14a_protectimus_nfc -t 2021-03-14T13:37:00+01:00
[+] executing lua
/home/matt/research/proxmark3/client/luascripts/hf_14a_protectimus_nfc.lua
[+] args '-t 2021-03-14T13:37:00+01:00'
[+] Found token with UID 3F10000323540E
[+] Set Unix time 1615725420
[!] Please power the token and press <ENTER>

[+] The future OTP on 2021-03-14T13:37:00+01:00 (1615725420) is 303831
[+] Set Unix time 1612451460

[+] finished hf_14a_protectimus_nfc


A SySS proof of concept video illustrating this security Vulnerability
is available on our SySS Pentest TV YouTube channel [5].

The developed Lua script for Proxmark3 is available on our GitHub
site [6].

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Solution:

SySS is not aware of a solution for the described security issue.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclosure Timeline:

2021-02-04: Vulnerability reported to manufacturer
2021-02-04: Manufacturer acknowledges receipt of security advisory and
             asks for further information
2021-02-05: SySS provides further information to manufacturer
2021-06-16: Public release of security advisory

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

References:

[1] Product website for Protectimus SLIM NFC
    https://www.protectimus.com/protectimus-slim-mini/
[2] Proxmark3 GitHub repository by the RFID Research Group
    https://github.com/RfidResearchGroup/proxmark3
[3] SySS Security Advisory SYSS-2021-007

https://www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-007.txt
[4] SySS GmbH, SySS Responsible Disclosure Policy
    https://www.syss.de/en/responsible-disclosure-policy
[5] SySS Proof of Concept Video: To the Future and Back - Attacking a
TOTP Hardware Token
    https://www.youtube.com/watch?v=C0pM6TIyvXI
[6] Protectimus SLIM NFC Lua script for Proxmark3
    https://github.com/SySS-Research/protectimus-slim-proxmark3
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Credits:

This security vulnerability was found by Matthias Deeg of SySS GmbH.

E-Mail: matthias.deeg (at) syss.de
Public Key:
https://www.syss.de/fileadmin/dokumente/Materialien/PGPKeys/Matthias_Deeg.asc
Key fingerprint = D1F0 A035 F06C E675 CDB9 0514 D9A4 BF6A 34AD 4DAB

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Disclaimer:

The information provided in this security advisory is provided "as is"
and without warranty of any kind. Details of this security advisory may
be updated in order to provide as accurate information as possible. The
latest version of this security advisory is available on the SySS website.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Copyright:

Creative Commons - Attribution (by) - Version 3.0
URL: http://creativecommons.org/licenses/by/3.0/deed.en
```


Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other
SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Login or Register to add favorites

packet storm
© 2022 Packet Storm. All rights reserved.

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter
Subscribe to an RSS Feed