LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

HC3 Intelligence Briefing "SweynTooth" Devices in the Medical Environment

OVERALL CLASSIFICATION IS

TLP:WHITE

3/19/2020

Agenda

- Overview
- HC3 Assesment
- Types of Devices Affected by “SweynTooth”
- Manufacturers Affected by “SweynTooth”
- 12 CVEs Disclosed by ASSET Researchers
- What Can Hackers do if Exploited?
- Other BLE Devices in Health Care Facilities
- Assessment / Mitigation
- References
- Questions

Slides Key:

	Non-Technical: managerial, strategic and high-level (general audience)
	Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Overview

Researchers at the Singapore University of Technology and Design identified over 12 vulnerabilities associated with Bluetooth Low Energy (BLE) devices:

- Some CVEs are undisclosed because of non-disclosure agreements
- Collectively referred to as the "SweynTooth" vulnerabilities
- Estimated that "millions" of logistics, medical, consumer electronic, smart home, and wearable BLE devices affected
- The vulnerabilities affect BLE wireless communication software development kits for 7 system-on-a-chip (SoC) manufacturers
- Exploitation → Crash and/or Deadlock and/or Security Bypass
- BLE devices are used for various functions in the day-to-day operations of a health care facility

SWEYNTOOTH

HC3 Assessment

HC3 Assessment – High Risk

- HC3 analysts assess with high confidence that there are devices affected by “SweynTooth” in most medical settings.
- Bluetooth devices that do not have an external power source and are designed for ‘prolonged battery life’ (rechargeable) likely use BLE SoCs that could potentially be affected by “SweynTooth”.
- **A mitigation is to turn Bluetooth off on devices if the functionality is not needed.**
- **If available by the manufacturer, the application of available patches for affected devices is the only known remediation for “SweynTooth”.**

Types of Devices Affected by "SweynTooth"

The vulnerabilities affect Bluetooth Low Energy (BLE) wireless communication software development kits, commonly used in devices such as "logistics, medical, consumer electronics, smart home, wearables":

- Fitness Bands
- Hearing Aids
- Bluetooth Headsets
- Bluetooth Trackers
- Remote Controls
- Virtual Reality
- Human Interface Device Profile (HID)
- Apple HomeKit
- Other rechargeable devices

(a) FitBit Inspire

(b) Eve Energy

(c) August Smart Lock

(d) CubiTag

(e) eGeeTouch

For more resources about medical device cybersecurity visit FDA.gov. Or contact the Division of Industry and Consumer Education or CyberMed@fda.hhs.gov.

Manufacturers Affected by "SweynTooth"

The researchers identified 480 vulnerable devices—the total number of affected devices is estimated to be in the millions—that use chips produced by seven system-on-a-chip (SoC) vendors:

1. Cypress
2. NXP
3. Dialog Semiconductors
4. Texas Instruments
5. Microchip
6. Telink Semiconductor
7. ST Microelectronics

12 CVEs Disclosed by ASSET Researchers

The 12 vulnerabilities disclosed were classified into three different "vulnerability types" by the researchers:

Type	Vulnerability Name	Affected Vendors	CVE
Crash	Link Layer Length Overflow	Cypress, NXP	CVE-2019-16336 CVE-2019-17519
	Truncated L2CAP	Dialog Semiconductors	CVE-2019-17517
	Silent Length Overflow	Dialog Semiconductors	CVE-2019-17518
	Public Key Crash	Texas Instruments	CVE-2019-17520
	Invalid L2CAP Fragment	Microchip	CVE-2019-19195
	Key Size Overflow	Telink Semiconductor	CVE-2019-19196
Deadlock	LLID Deadlock	Cypress, NXP	CVE-2019-17061 CVE-2019-17060
	Sequential ATT Deadlock	STMicroelectronics	CVE-2019-19192
	Invalid Connection Request	Texas Instruments	CVE-2019-19193
Security Bypass	Zero LTK Installation	Telink Semiconductor	CVE-2019-19194

What Can Hackers do if Exploited?

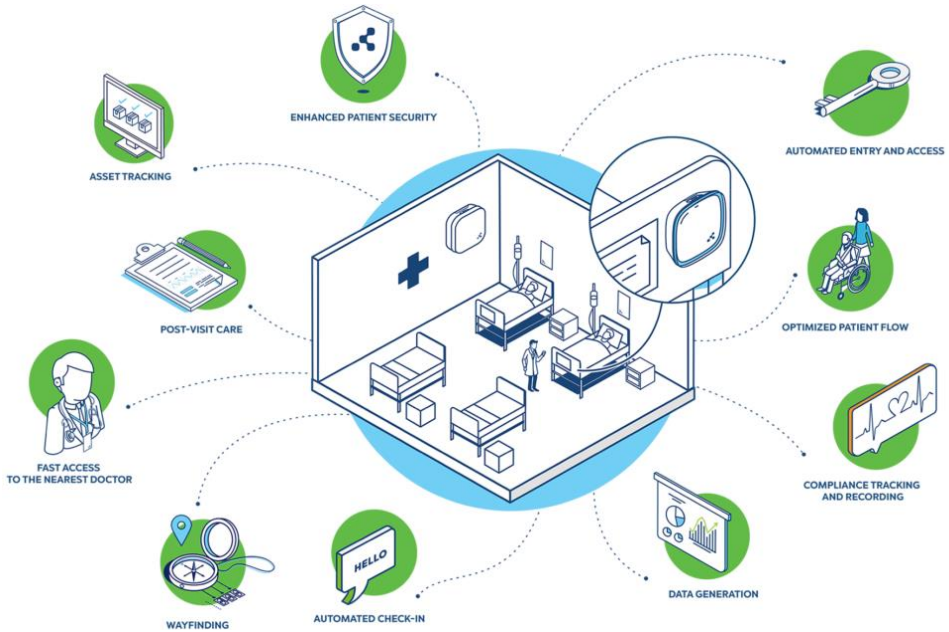
Type	Vulnerability Name	Impact
Crash CVEs: **CVE-2019-16336** **CVE-2019-17519** **CVE-2019-17517** **CVE-2019-17518** **CVE-2019-17520** **CVE-2019-19195** **CVE-2019-19196**	Link Layer Length Overflow	• Trigger a buffer overflow (Denial of Service) • Cause the device to restart • Possible remote execution • Force user to restart device (remove “deadlock” state of device) • Bypass encryption and leak user information
	Truncated L2CAP	
	Silent Length Overflow	
	Public Key Crash	
	Invalid L2CAP Fragment	
	Key Size Overflow	
Deadlock CVEs: **CVE-2019-17061** **CVE-2019-17060** **CVE-2019-19192** **CVE-2019-19193**	LLID Deadlock	• Deny/disrupt the BLE connection • Cause the device to restart • Force user to restart device (remove “deadlock” state of device)
	Sequential ATT Deadlock	
	Invalid Connection Request	
Security Bypass CVE: **CVE-2019-19194**	Zero LTK Installation	• Give the attacker read/write access to the victims device

Other BLE Devices in Health Care Facilities

BLE-enabled devices in the medical environment could be devices that transmit data from the device—such as stethoscopes glucose monitors, scales, and pulse readers—to smartphones or tablets. Beyond individual devices used for patient assessments, Bluetooth devices are used for various functions in the day-to-day operations of a health care facility for: *

- Asset Management
- Automated Check-In
- Automated Physical Entry and Access
- Blood Transport Tracking
- Compliance Tracking and Recording
- Data generation
- Patient Security/Doctor Response
- Environmental Monitoring
- Optimized Patient Flow

* Non-Exhaustive List



Smart Hospital with Bluetooth Beacons

Assessment / Mitigation

Assessment – High Risk

- HC3 analysts assess with high confidence that there are devices affected by "SweynTooth" in most medical settings.
- Because researchers have not yet disclosed the additional vulnerable SoCs and some security companies have placed the number of devices in the millions, there is a high likelihood of an affected device being present in most medical environments.
- Individual organization's risk depends on the device(s) targeted:
  - PII or Patient Medical Device?

Mitigation

- Identification of Devices Potentially Affected by "SweynTooth"
  - Bluetooth devices that do not have an external power source and are designed for 'prolonged battery life' (rechargable) likely use BLE SoCs.
- Identification of the SoCs used by those BLE devices
  - Necessary to determine the risk posed to the user's organization
- If available by the manufacturer, the application of available patches for affected devices is the only known mitigation for "SweynTooth".
  - SoC manufacturers Cypress, NXP, Texas Instruments, and Telink have released patches for affected devices. By the end of March, Dialog will have patches available for affected devices.

Mitigation Practices: "SweynTooth" Devices

The HHS 405(d) Program published the Health Industry Cybersecurity Practices (HICP), which is a free resource that identifies the top five cyber threats and the ten best practices to mitigate them. Below are the practices from HICP that can be used to mitigate:

DEFENSE/MITIGATION/COUNTERMEASURE	405(d) HICP REFERENCE
Implement information security assurance practices, such as security risk assessments of new devices and validation of vendor practices on networks or facilities	**[1.L.A]**
Implement pre-procurement security requirements for vendors	**[9.L.C]**
Patch devices after patches have been validated, distributed by the medical device manufacturer, and properly tested	**[9.M.B]**
Establish and maintain communication with medical device manufacturer's product security teams.	**[9.L.A]**

- FDA Informs Patients, Providers and Manufacturers About Potential Cybersecurity Vulnerabilities in Certain Medical Devices with Bluetooth Low Energy
  - https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0
- ICS Alert (ICS-ALERT-20-063-01) SweynTooth Vulnerabilities
  - https://www.us-cert.gov/ics/alerts/ics-alert-20-063-01

Background information can be found here:
https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

References

- ASSET Research: Unleashing Mayhem over Bluetooth Low Energy
  - https://asset-group.github.io/disclosures/sweyntooth/
- Dialog Semiconductor: Wearables
  - https://www.dialog-semiconductor.com/products/connectivity/bluetooth-low-energy/applications/wearable
- Bitdefender: Millions of Bluetooth Devices Affected by SWEYNTOOTH Vulnerabilities
  - https://www.bitdefender.com/box/blog/iot-news/millions-bluetooth-devices-affected-sweyntooth-vulnerabilities/
- Orthogonal: The Growing Significance of Bluetooth BTLE in Healthcare
  - https://orthogonal.io/insights/the-growing-significance-of-bluetooth-btle-in-healthcare-html/
- Kontakt.io: 15 Top Bluetooth-Based IoT Uses in Healthcare
  - https://kontakt.io/blog/10-top-bluetooth-tag-uses-in-healthcare/
- Medical Device Cybersecurity: What You Need to Know
  - https://www.fda.gov/consumers/consumer-updates/medical-device-cybersecurity-what-you-need-know

Questions

Upcoming Briefs

- Multifactor Authentication
- Cybersecurity Implications for Telework in HPH

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to **HC3@HHS.GOV**.

Requests for Information

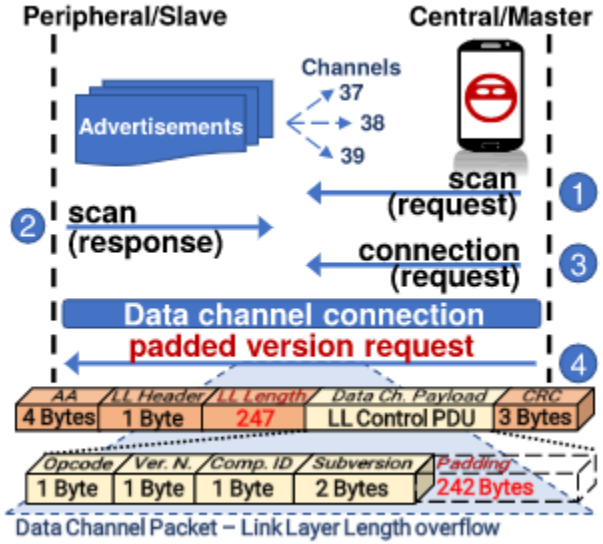
Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

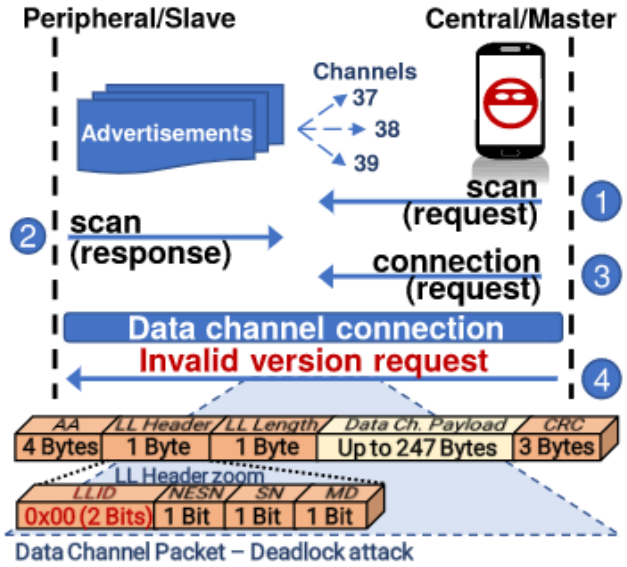
Appendix

What Can Hackers do if Exploited? (cont.)

Link Layer Length Overflow - CVE-2019-16336, CVE-2019-17519

- Allows attackers in radio range to trigger a **buffer overflow** by manipulating the LL Length Field, primarily leading to a **denial of service attacks**.





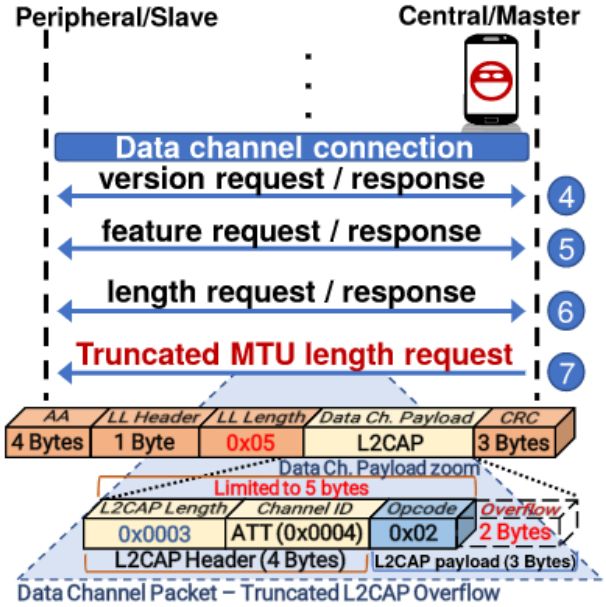
Link Layer LLID deadlock - CVE-2019-17061, CVE-2019-17060

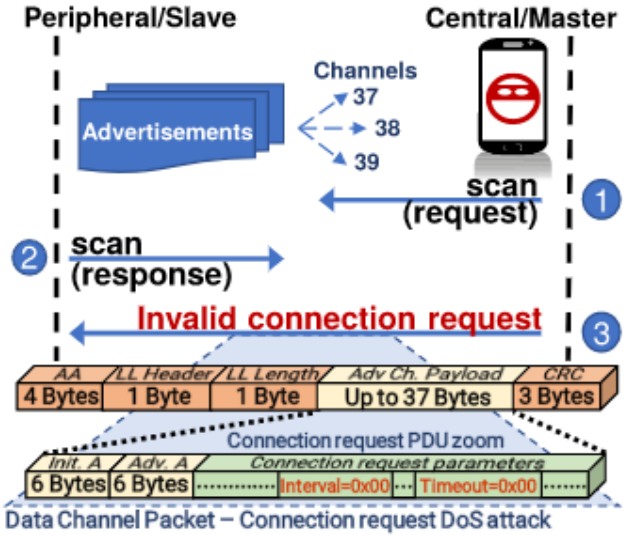
- These **trigger deadlock state** when a device receives a packet with the LLID field cleared.

What Can Hackers do if Exploited? (cont.)

Truncated L2CAP - CVE-2019-17517

- This flaw results due to a lack of checks while processing an L2CAP packet, causing a **denial of service and crash** of the device.





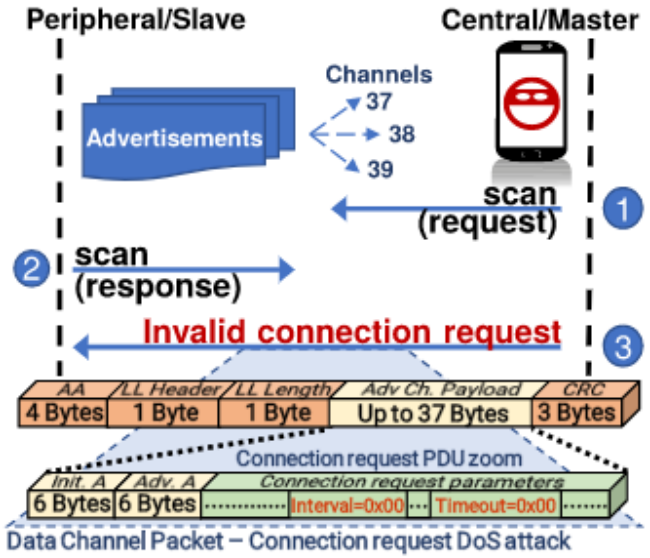
Silent Length Overflow CVE-2019-17518

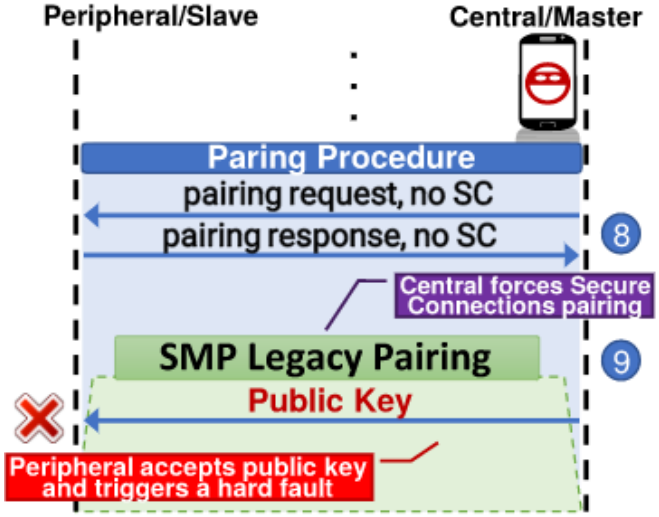
- A **buffer overflow** occurs when a certain packet payload with higher than expected LL Length is sent, the **peripheral crashes**.

What Can Hackers do if Exploited? (cont.)

Invalid Connection Request - CVE-2019-19195

- When devices do not properly handle some connection parameters while the central attempts a connection to the peripheral, they could lead to **Deadlock state**.





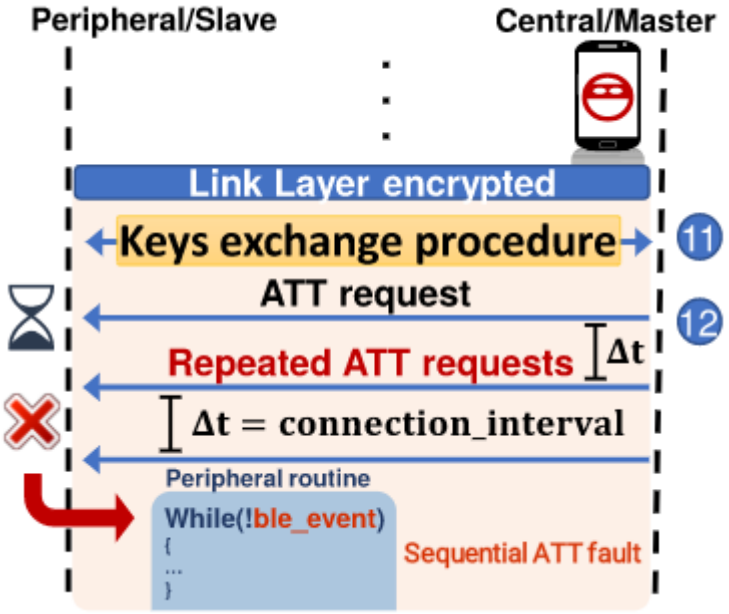
Unexpected Public Key Crash - CVE-2019-17520

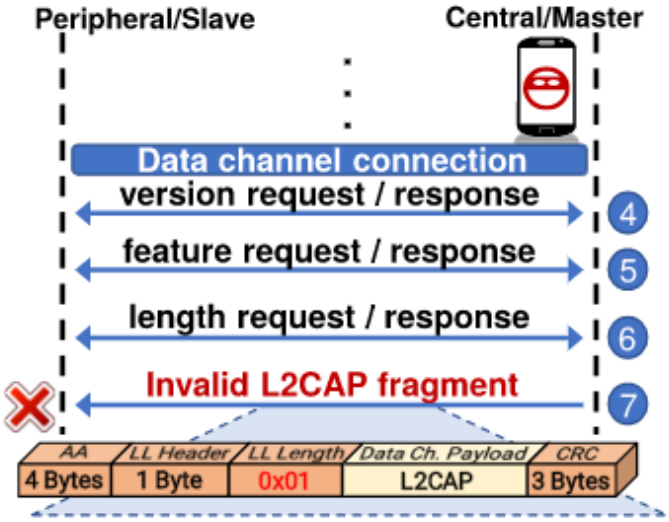
- This bug is present in the implementation of the legacy pairing procedure, which is handled by the Secure Manager Protocol (SMP) implementation and can be used to perform **DoS and possibly restart products**.

What Can Hackers do if Exploited? (cont.)

Sequential ATT Deadlock - CVE-2019-19192

- This flaw lets attackers **deadlock the peripheral** by sending just two consecutive ATT request packets in each connection event.





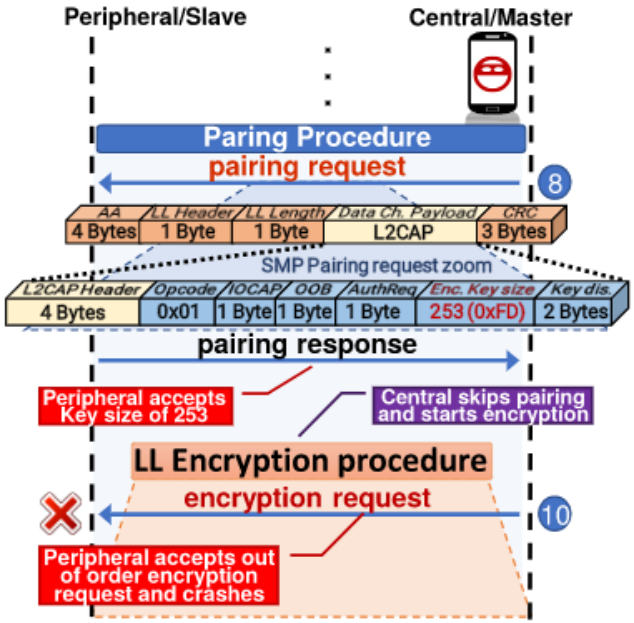
Invalid L2CAP fragment - CVE-2019-19195

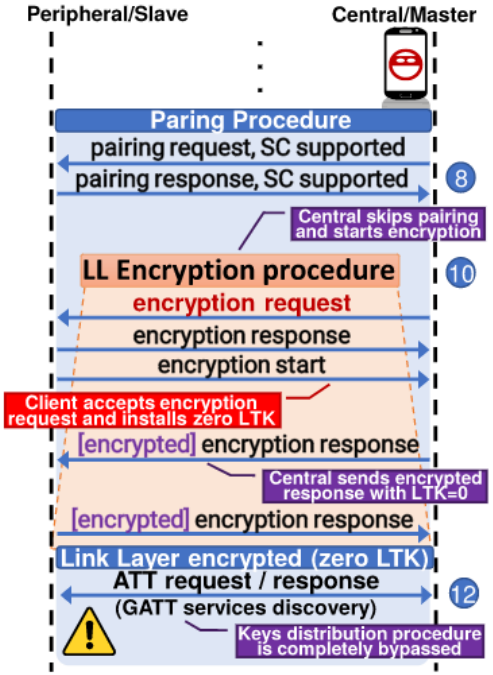
- Improper handling of the PDU size of the packets can lead to **deadlock behavior**.

What Can Hackers do if Exploited? (cont.)

Key Size Overflow - CVE-2019-19196

- This overflow in the device memory issue is a combination of multiple bugs found during the pairing procedure of devices, **resulting in a crash**.





Zero LTK Installation - CVE-2019-19194

- This critical vulnerability is a variation of one of the Key Size Overflow. It affects all products using Telink SMP implementation with support for secure connection enabled and can give an attacker **read/write access** to the victims device.