BadUSB-C: Revisiting BadUSB with Type-C

Hongyi Lu, Yechang Wu, Shuqing Li, You Lin, Chaozu Zhang
Fengwei Zhang

Southern University of Science and Technology

May 28, 2021
Outline

1. Background
2. Design & Prototype
3. Case Study
4. Limitations
5. Mitigation & Responsible Disclosure
6. Conclusion
The Ubiquitous Peripheral

HIDs
The Ubiquitous Peripheral

Charging
The Ubiquitous Peripheral

Data Transfer
All in One With Type-C
All in One With Type-C
### BadUSB-C: Revisiting BadUSB with Type-C

#### Background

**USB Vulnerabilities**

With Great Power Comes Great Responsibility

<table>
<thead>
<tr>
<th>Year</th>
<th>Version</th>
<th>Peripherals</th>
<th>Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1996</td>
<td>USB 1.x [1, 2]</td>
<td>Keyboard, Mouse...</td>
<td>BadUSB [3]...</td>
</tr>
<tr>
<td>2000</td>
<td>USB 2.0 [4]</td>
<td>Flash Drive, CD Driver...</td>
<td>/</td>
</tr>
<tr>
<td>2008</td>
<td>USB 3.0 [5]</td>
<td>/</td>
<td>/</td>
</tr>
<tr>
<td>2013</td>
<td>USB 3.1 [6]</td>
<td>DisplayPort, ThunderBolt...</td>
<td>BadUSB-C</td>
</tr>
<tr>
<td>2017</td>
<td>USB 3.2 [7]</td>
<td>/</td>
<td>/</td>
</tr>
</tbody>
</table>

USB Protocol Timeline.
Traditional BadUSB

I'm a keyboard

USB Flash Drive

OK!

Victim's Device

Traditional BadUSB Attack.
Traditional BadUSB

"/bin/bash ..."

USB Flash Drive

Victim's Device

Traditional BadUSB Attack.
Traditional BadUSB

No Feedback? Why?

USB Flash Drive

Victim's Device

Traditional BadUSB Attack.
BadUSB Limitations

There are some limitations of the traditional BadUSB attack.

- Cannot perform attack precisely.
- Cannot interact with GUI.
- Require host network usage.
Overview

1. Victim’s Devices
2. BadUSB-C
3. Attacker’s Remote PC

Diagram showing the flow of information between Victim’s Devices, BadUSB-C, and Attacker’s Remote PC.
Video Path

1. Victim’s Devices
2. BadUSB-C
3. Attacker’s Remote PC
HID Path

1. Victim’s Devices
2. BadUSB-C
3. Attacker’s Remote PC
Individual WiFi/GSM

1. Victim’s Devices
2. BadUSB-C
3. Attacker’s Remote PC
Prototype

A  Victim’s Device
1  USB 3.x Hub
3  Auxiliary Power Bank
5  ATMEGAA32U4 Board

B  BadUSB-C
2  Raspberry Pi 4B
4  Video Capture
Sharing Powerbank

Low Power

Sharing Powerbank
Typical Attack Procedure

1. The attacker rents a power bank and replaces the internal components with BadUSB-C.
2. An attacker-crafted power bank is returned to the rental station in crowded areas.
3. A user borrows the modified power bank and connects it to his/her own device.
4. The attacker can now fully control the victim’s device.
We conducted experiment on a HUAWEI P30 Android smartphone. Eleven applications were selected and tested in the following steps:

1. Login in with a test account.
2. Keep the default settings.
3. Attach BadUSB-C to the test device.
4. Simulate victim’s daily usage of the application.
Experiment Screenshots
### Experiment Result

<table>
<thead>
<tr>
<th>Application</th>
<th>Leaked Sensitive Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>WeChat</td>
<td>Financial Status, History, Payment QR Code</td>
</tr>
<tr>
<td>WhatsApp</td>
<td>Contacts, Chat History, Phone Number</td>
</tr>
<tr>
<td>Alipay</td>
<td>Financial Status, Payment QR Code</td>
</tr>
<tr>
<td>Paypal</td>
<td>Paypal Balance</td>
</tr>
<tr>
<td>Health</td>
<td>Personal Health Metrics</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
BadUSB-C: Revisiting BadUSB with Type-C

Limitations

BadUSB-C also has several limitations.

- Cannot bypass biometrics authentications like fingerprint.
- Requires the DisplayPort over USB Type-C feature to work.
- May incur notifications on victim’s devices and be discovered.
BadUSB-C: Revisiting BadUSB with Type-C
Mitigation & Responsible Disclosure

Isolated UI Rendering

Sensitive Layer

Insensitive Layer

Untrusted Screen

Trusted Screen

Isolated UI Rendering
We contacted HUAWEI after we discovered this vulnerability, who later assigned a CVE entry (CVE-2021-22325) for this vulnerability.

HUAWEI Response

为了确保安全漏洞的及时修复，我们建议您尽快更新至最新版本。关于漏洞的详细信息，请参阅以下链接：https://consumer.huawei.com/en/support/bulletin/2021-3。相关CVE编号为：CVE-2021-22325

CVE-2021-22325: Video streaming vulnerability in some Huawei phones
Severity: Medium
Affected versions: EMUI 11.0.0, Magic UI 4.0.0
Impact: Successful exploitation of this vulnerability may result in video streams being intercepted during transmission.

同时，该漏洞符合华为终端安全漏洞奖励计划规则，且已经通过评审。我们将会在5月底支付该漏洞奖金，编号为：HWSA21-0696562357。详细进展请通过https://bugbounty.huawei.com查看

致

华为PSIRT
We also applied for the bug bounty program of HUAWEI and gained a reward of over $4500.

**Vulnerability Name:** USB-C Video Stream Leakage

**Vulnerability Type:** Mobile/Info Leakage

**Vulnerability Status:** Confirmed

**Vulnerability Level:** High

**Bounty:** 4500$
Now, mitigation for this vulnerability has already been deployed.

This mitigation requires user authentication before allowing external USB devices.
Conclusion

We summarize our work as follows.

1. We explore a new attack scheme leveraging the latest feature of USB protocol.
2. We conduct real-life scenario study of sharing powerbank to test BadUSB-C efficiency.
3. We propose novel mitigation for our BadUSB-C attack.
Thank You!

{11712009,11711918,lisq2017,11711809,11712021}@mail.sustech.edu.cn
zhangfw@sustech.edu.cn


Conclusion