

---

**Subject:** RE: [EXT] Re: CVE Request 904700 for CVE ID Request  
**Date:** Wednesday, March 31, 2021 at 07:08:01 Hong Kong Standard Time  
**From:** CVE Request  
**To:** mobitec@ie.cuhk.edu.hk, CVE Request

Regarding your CVE Request 904700 for CVE ID.

Expect the CVE entries mentioned in this email to be updated on <http://cve.mitre.org> in the next few hours.

CVE's that are **\*\* RESERVED \*\*** will remain in a pending state until we are provided with at least one public reference that follows the CVE Entry Reference Requirement rules in section 8.3 ([https://cve.mitre.org/cve/cna/rules.html#section\\_8-3\\_cve\\_entry\\_reference\\_requirements](https://cve.mitre.org/cve/cna/rules.html#section_8-3_cve_entry_reference_requirements)).

When the candidates are publicized, please send us the link to the advisory using <https://cveform.mitre.org> with "Notify CVE about a publication" as the request type.

-----  
[VulnerabilityType Other]  
CWE-347: Improper Verification of Cryptographic Signature

-----  
[Additional Information]  
We have prepared a vulnerability report at [https://www.dropbox.com/s/czbkdr73tclq2nr/UnionPay\\_Vulnerability\\_Report.txt?dl=0](https://www.dropbox.com/s/czbkdr73tclq2nr/UnionPay_Vulnerability_Report.txt?dl=0). We set up a merchant server by ourselves using the vulnerable SDK at <http://18.140.73.64/> for a PoC. Besides, we write a PoC script to attack our own merchant server, which is available at [https://www.dropbox.com/s/6smwnbrp0kgsgrc/poc\\_code.py?dl=0](https://www.dropbox.com/s/6smwnbrp0kgsgrc/poc_code.py?dl=0).

-----  
[Affected Component]  
signature verification function, i.e., validate(), within the vulnerable SDK for handling the payment results from UnionPay's cashier server

-----  
[Attack Type]  
Remote

-----  
[CVE Impact Other]  
The vulnerability enables the attacker to shop for free in merchants' websites and mobile apps, whose servers use the

payment services from UnionPay.

---

[Attack Vectors]

To

exploit the vulnerability, the attacker needs to forge a payment notification, whose message authentication code (MAC) is generated based on a secret key of NULL. After that, the attacker can impersonate as the UnionPay's cashier server and send the message to the notification URL hosted by the merchant server. Consequently, the merchant server will be cheated and enable the attacker to shop for free.

---

[Discoverer]

Shangcheng SHI, Mobile Technologies Centre (MobiTeC, <http://mobitec.ie.cuhk.edu.hk>), Department of Information Engineering, The Chinese University of Hong Kong

---

[Reference]

<http://mobitec.ie.cuhk.edu.hk> <http://unionpay.com>  
<https://open.unionpay.com/tjweb/acproduct/list?apiSvcId=448&index=4>  
[https://www.dropbox.com/s/6smwnbrp0kgsgrc/poc\\_code.py?dl=0](https://www.dropbox.com/s/6smwnbrp0kgsgrc/poc_code.py?dl=0)  
[https://www.dropbox.com/s/czbkdr73tclq2nr/UnionPay\\_Vulnerability\\_Report.txt?dl=0](https://www.dropbox.com/s/czbkdr73tclq2nr/UnionPay_Vulnerability_Report.txt?dl=0)

---

[Vendor of Product]

UnionPay

---

[Affected Product Code Base]

UnionPay PHP SDK (for online payment) UnionPay does not assign Version ID for its SDKs, but they are available online, e.g.,

<https://open.unionpay.com/tjweb/acproduct/list?apiSvcId=448&index=4> &  
<https://open.unionpay.com/upload/download/%E7%BD%91%E5%85%B3%E6%94%AF%E4%BB%98%E4%BA%A7%E5%93>

Use CVE-2020-23533 for:

\*\* RESERVED \*\* Union Pay up to 1.2.0, for web based versions contains a CWE-347:

Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which

is generated based on a secret key which is NULL.

Use CVE-2020-36284 for:

**\*\* RESERVED \*\*** Union Pay up to 3.4.93.4.9, for android, contains a CWE-347: Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which is generated based on a secret key which is NULL.

Use CVE-2020-36285 for:

**\*\* RESERVED \*\*** Union Pay up to 3.3.12, for iOS mobile apps, contains a CWE-347: Improper Verification of Cryptographic Signature vulnerability, allows attackers to shop for free in merchants' websites and mobile apps, via a crafted authentication code (MAC) which is generated based on a secret key which is NULL.