New issue

Jump to bottom

# Public disclosure on CVE-2020-8818 [Unauthorized Payments Hijacking + Order Status Spoofing] #54

Closed **633kh4ck** opened this issue on Feb 24, 2020 · 1 comment

**633kh4ck** commented on Feb 24, 2020 • edited

## CVE-2020-8818

Lack of origin authentication (CWE-346) at IPN callback processing function allow (**even *unauthorized***) attacker to remotely replace critical plugin settings (merchant id, secret key etc) with known to him and therefore bypass payment process (eg. spoof order status by manually sending IPN callback request with a valid signature but without real payment) and/or receive all subsequent payments (on behalf of the store).

### Vulnerable code (fixed in PR #53)

magento2/Controller/Payment/Callback.php
Lines 88 to 107 in 715979e

```
88      if (!empty($get['cgp_sitesetup']) && !empty($get['token'])) {
89
90              try {
91                      $bIsTest = ($get['testmode'] == 1 ? true : false);
92                      $aResult = $this->_cardgateClient->pullConfig($get['token'], $bIsTest);
93                      $aConfigData = $aResult['pullconfig']['content'];
94                      $this->_cardgateConfig->setGlobal( 'testmode', $aConfigData['testmode'] );
95                      $this->_cardgateConfig->setGlobal( 'site_id', $aConfigData['site_id'] );
96                      $this->_cardgateConfig->setGlobal( 'site_key', $aConfigData['site_key'] );
97                      $this->_cardgateConfig->setGlobal( 'api_username', $aConfigData['merchant_id'] );
98                      $this->_cardgateConfig->setGlobal('api_password', $this->encryptor->encrypt($aConfigData['api_key'] ));
99                      $typeListInterface = ObjectManager::getInstance()->get( \Magento\Framework\App\Cache\TypeListInterface::class );
```

**Affected versions:** ≤ 2.0.30
**Tested on:** Magento 2.3.4 + CardGate Payment Gateway Module 2.0.30

▶ **Proof-of-Concept**

👍 3 🎉 1 🚀 1 👀 1

**cardgate** commented on Mar 2, 2020 • edited Owner

CardGate would like to thank Vladislav Svolsky @633kh4ck for pointing out this vulnerability to us and allowing us the time to implement a fix before this public disclosure.
Because we have also made changes on the gateway, it is no longer possible to exploit this vulnerability.
This also applies to all our extensions with versions <= 2.0.30, so **all existing implementations are now no longer vulnerable**.

The basic problem was located in a function to automatically configure the webshop plugin with the push of a button in the CardGate back office.
We would like to emphasise that this convenience functionality is now only supported for the latest plugin version and will not work for earlier versions.

**cardgate** closed this as completed on Mar 2, 2020

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

2 participants