

Regulus Exposed

by: Masood Mehmood, 09/16/2004

<http://www.securitydocs.com/library/2547>

Introduction

Regulus is a real-time monitoring / accounting / billing software package available at <http://www.safe.ca/>. Mostly use by ISP to manage their users by creating logs, restrictions, usages and timing. Regulus contains two programs, one you can say front end and the other one is back end. Front end program contains PHP stuff and back end for disconnections or making low level actions. And it is quite good in performing certain tasks like.

- The user account has expired or is terminated.
- The customer is using your resources after the grace period allowed to pay his contract.
- The user has used all his available time or bandwidth on the network.
- The user has no right to access the network for the current period of the day.
- There are too many users using that same ID on that account.
- There are too many users connected on that contract.
- A staff operator has requested that the user be disconnected.
- The user has an uncommitted contract and lines are needed for committed customers.
- The user has reached his maximum session time.

This package needs a license but you can get its evaluation version and do study as I did.

Regulus

After installation Regulus creates four virtual domains.

1. cust.domain
2. acct2.domain
3. access.domain
4. registry.domain

All these Virtual domains do different works like cust.domain is use for customer interactions . acct2.domain is use for staff member access. access.domain just to hold you on root directory. registry.domain is use for updating user accounts.

Bugs

Regulus is useful and easy to use RADIUS software but it contains following bugs.

1. Default DES encryption.
2. Easy to obtain any user information (such as password, personal information etc...)
3. Staff File Default path.
4. Poor Authentication procedure.
5. Any miss-configuration exposed all system.

DES

DES uses 56 bits of encryption and considerably easy to crack. DES limits its passwords length to 8 characters. I think having MD5 facility available with more strong encryption, MD5 should be its default encryption technique. John The Ripper or cracker jack are quite good in breaking DES

encryption. And most of the Administrator and users dont use strong password and thats what make carker's work easy.

Users Information

Well this is the weakest point or you can call it the poor programming approach. When you first interact with regulus the first page you going to have is

http://cust.domainname/

Here you have to put your user name and password. It seems all fine, you will have all correct information about your account and usage details. But we are not dealing with correct information. The question here is any one without having my password can see what I am looking? The answer is yes. And he can change password, use your account etc..

Exploiting this hole is very easy just follow my instructions

"http://cust.domain/base-dir/htmlcust/custchoice.php?lang=English&userid=&action=To see your connections logs"

Now in-place of you can put any user name any card number and you will get all information like you are in with the password. The main reason of this is not that I am smart enough, well the reason is poor Regulus programming and that's what I want to show you in this paper.

Password

Now not only this you can change password. HOW?? Simple change its one parameter to

http://cust.domain/base-dir/htmlcust/custchoice.php?lang=English&userid=&action= To update your password

Now that's simple but it require old password as well, at this point Regulus creator must be thinking they did a great job but if we view the source code of that page that old password is available in hidden tags but in encrypted form. Now we can do 2 things here change the password or copy the encrypted password and break that using password creator tools....

Changing password

I don't know why they give password in hidden tags while using great PHP. Simple look at this << iiTQ1mHn1.vQ >> this is an encrypted form of 123 using DES.. Now how to use it.

Save that Password update page and fill in that hidden tags of OLD password with your encrypted password and save that page. You can follow the following method as well.

*http://cust.domain/base-dir/htmlcust/custpass.php?
lang=English&base=/var/lib/regulus2&pass=iiTQ1mHn1.vQ&userid=&old
pass=123&newpass1=&newpass2=&action=update*

Just give new password 2 times with old password as the above-encrypted form and you will see this

The password provided is OK and will be shortly stored in our Data-Base

Well that's great.

Hacking Staff Users to Get Control Over Regulus

Simple as u ever think of, try this

<http://cust.domainname/base-dir/access/stafffile>

So you got password list hmmmhhh again DES. Cracking require time but as I said people don't use strong password because they can't even remember them self:).

After Getting the password try this link

<http://acct2.domainname/>

Give user name and password and you will say hmmmhhh Regulus is so easy to use hehehe So I think one credit goes to Regulus is that it is easy to use. I have a practical example of what I explained above, although the name of that ISP is hidden.

<http://www.aosp.net/regulus.ppt>

Hidden Bugs

There are so many other bugs that are still hidden but I am after them as well. and most of them are already secured by REGULUS TEAM and all these bugs are already send to them. A bug which expose all system uses access.domaain/etc/passwd is still hidden but my ISP do have this bug.

Testing

Regulus security against SQL-Injections, Buffer Overflows is quite good and I am still testing other stuff.

Masood Mehmood

{ PHClub Reaserch Works }

Email= masud.sp@gmail.com

<http://www.phclub.org>