

Forum:[Hack Forums](#)

Thread: [GameCP Oday local root exploit](#)

Starfall - February 16, 2013, 2:07 pm

Code <Starfall> Hi, are any GameCP coders here? I'd like to discuss a sensitive issue.

<Starfall> okay, sorry but i gotta do this

<Starfall> Billy N00kstrr Uf0 Adzgibbo|H Archey brayden_ Clinton Daniel0 davidbanham Jackster_Williamji7

<Jackster_> Grow up

<Jackster_> Need to talk to staff then email

<Jackster_> don't come here spamming

<Starfall> a single line is spamming, makes perfect sense

<Starfall> get over yourself, I'm trying to help fix an exploitable bug but you just fucked it up for everybody

<Starfall> now it's going on Full Disclosurre

<Jackster_> Then email support

<Starfall> nope, too late, the skiddies get it now

<Jackster_> right...

<Starfall> IRC is supposed to be a more immediate support channel, and I figured that due to the nature of the issue I should try here first. Is there a problem with that?

<Jackster_> Sunday night

<Starfall> I said, is there a problem with that? Not "what day is it"

<Starfall> You have one hell of an attitude towards people trying to help, and I sincerely hope you're not on the GCP support team.

<Jackster_> Sunday night as in the staff are not in the office

<Jackster_> You are not asking for support

<Starfall> I am asking them to fix an issue, is that not support?

<Jackster_> if you have found a problem then either email support or add it to the bugs.gamecp.com

<Starfall> Due to many spammers abusing our bugs system we have temporarily disabled it while we increase spam prevention.

<Starfall> If you have a bug email it to support@gamecp.com

<Starfall> I've already sent one email by the way. Stop being such a stuck up asshole when someone wants to fix something.

<Starfall> I'm emailing FD now, have fun cleaning up the mess.

<Jackster_> oh grow up kiddo This exploit is simple. You create a plugin for whatever game is running on the panel that creates a symlink to /etc/shadow, use the built in file manager to edit the symlink and change root's password and log in. Game over.

There is no need for a POC here. Instructions are detailed enough. The spoiler below is just a silly, slightly-relevant thing.

Oh and by the way, Jackster got banned from that IRC about 2 hours later for being an asshole and impersonating staff.

This is the last time I ever try to whitehat anything, even boring worn-out bugs like this one.

Spoiler ([Click to View](#))

This is my war song all for you

I just do not know what to do

I keep on coming back it's true

At 10 I knew my place was here

So leave your doubts and have no fear
The righteous path is clear

Pay me no heed I'm about to cause a shakeup
Why won't you just wake up
Why can't you just take up
Arms to defend yourself against me?
Dashing young rogues can't be helped when consecrated
I still stand elated
Even when berated
Wish you could just see what I see
The gates have opened once again
A winter valley, summer sand
And all my friends, they tell me

Yeah, you got class
Yeah, you got style
How will you make it at 85?
This world's a battleground
You're lucky, even now, to be alive
From the ruins to the flag
I'll take it back I'll strike you down
I'll strike you down

Under-geared everywhere I look around me
Gnomes can still astound me
Trying to confound me
We don't have this problem, but you do
Excuse me miss, but I'd like to cash my honor
Thought I was a goner
Should have done a runner
But I still stood and fought for you

From the ruins to the flag
I'll take it back I'll strike you down
I'll strike you down

Tol Barad
It ain't so bad
Surrounded by my friends
Brave the weather
Fight the storm
Stay together
Live once more
Overpowered, my desire
Is to meet you in that spire
I'm on fire, can't cool down, oh can't you see?
It means too much to me
My life is PVP

?Hycca - February 16, 2013, 2:08 pm

Why did you delete your thread and re-post it? But nice Oday bby.

LevelUp - February 16, 2013, 2:09 pm

Did you not already post this earlier?

Nevertheless, fuck whitehat shit. You tried to do the right thing and this happens.

Also I didn't know you played WoW?

Starfall - February 16, 2013, 2:11 pm

(Feb 16, 2013 03:08 PM)?Hawkode Wrote: [\[CITE\]](#) Why did you delete your thread and re-post it? But nice Oday bby.

I didn't. Paradoxum did because you guys couldn't stay on topic.

Phizo - February 16, 2013, 2:24 pm

Nice job finding this.

Jackster is gay.

Light Yagami. - February 16, 2013, 4:45 pm

Nice job finding this starfall and sorry you had to repost it.

Gpure - February 16, 2013, 5:37 pm

I like the idea to white-hat it, but you did the right thing if the security team won't respond to a serious bug.

Jack Bauer - February 16, 2013, 5:38 pm

Good job dude! :) its nice to have people like you. :D

Starfall - February 16, 2013, 5:42 pm

(Feb 16, 2013 06:37 PM)Gpure Wrote: [\[CITE\]](#) I like the idea to white-hat it, but you did the right thing if the security team won't respond to a serious bug.I used to only whitehat stuff I didnt care about anymore.

Now, I whitehat nothing, because fuck you.

Dyme - February 16, 2013, 5:45 pm

Thanks ball of star I will use dis to own as many gibsons possible.