

Forum:[Hack Forums](#)

Thread: [O'boy look at dis beautiful .gov coldfusion vuln!](#)

Becky G - June 17, 2013, 1:52 pm

<https://www.newbedford-ma.gov/CFIDE/administrator/enter.cfm>

MiRP_Anon - June 17, 2013, 1:53 pm

You found a login page? Congrats /sarcasm

Becky G - June 17, 2013, 1:56 pm

It's coldfusion 8 you have a 30 second time frame to take the salt and password encrypt it to HMAC and then use it to log into the panel, jackass.

Cognitive - June 17, 2013, 1:57 pm

(Jun 17, 2013 01:56 PM)lordsql Wrote: [\[CITE\]](#) It's coldfusion 8 you have a 30 second time frame to take the salt and password encrypt it to HMAC and then use it to log into the panel, jackass. Then do it? It's not impressive unless you actually exploit it.

Becky G - June 17, 2013, 1:59 pm

I gave it away, and cold fusion is not very impressive. If you guys literally can't figure it out then i think you guys are half minded, I was expecting a "Thanks for the vuln .gov" or something. And i can't just give a login for it because the vuln changes every 30 seconds to a different HMAC.

For people who have no clue what is even going on or that need a guide for this for some reason...
http://www.blackhatlibrary.net/Coldfusion_hacking

Flaaffy - June 17, 2013, 2:01 pm

Thanks for the vuln .gov!

but guess what, i dont give a shit! find a vulnerability in cisco and then i will be impressed!

Cognitive - June 17, 2013, 2:03 pm

(Jun 17, 2013 01:59 PM)lordsql Wrote: [\[CITE\]](#) I gave it away, and cold fusion is not very impressive. If you guys literally can't figure it out then i think you guys are half minded, I was expecting a "Thanks for the vuln .gov" or something. And i can't just give a login for it because the vuln changes every 30 seconds to a different HMAC.

For people who have no clue what is even going on or that need a guide for this for some reason...
http://www.blackhatlibrary.net/Coldfusion_hacking

Never said I didn't understand the vulnerability. I'm saying how come you don't exploit it yourself, and show you did it? It's one thing to find vulnerabilities, but another to exploit them.

Becky G - June 17, 2013, 2:05 pm

1. I don't post what I do because i don't post stuff to you guys of what I do because no one needs to know what I do

2. This was a freebie for you guys

You guys try to defend yourselves so much when the only person that i had anger directed towards was MiRP. I didn't post this the rip on Hf, and you guys are just anger posting as if I was directing my post towards you.

Han. - June 17, 2013, 2:07 pm

By the way you're dodging it and changing the subject, you're clearly not able to exploit it.

Pendragon - June 17, 2013, 2:07 pm

(Jun 17, 2013 02:03 PM)Vitanis Mate Wrote: [\[CITE\]](#) Never said I didn't understand the vulnerability. I'm saying how come you don't exploit it yourself, and show you did it? It's one thing to find vulnerabilities, but another to exploit them.

He didn't exploit it and "gave it away" because it's patched. He can't exploit it.

Adobe has released patches for everything < CF9 regarding the LFD in the login panel.

Becky G - June 17, 2013, 2:11 pm

Wow this forum post turned into idiocy. .gov websites are not anything to be proud of on Hf these days nor do people get any props for finding them, so i just posted the vuln.

Andrew Downsend - June 17, 2013, 2:13 pm

Thanks for the vuln, exploited with no issues. Good job OP.

Becky G - June 17, 2013, 2:15 pm

Np. I just don't see why people went crazy over this easy vuln.

The Fail Collective - June 17, 2013, 2:30 pm

(Jun 17, 2013 02:13 PM)Andrew Downsend Wrote: [\[CITE\]](#) Thanks for the vuln, exploited with no issues. Good job OP.

Are you sure? I mean... are you really sure?

Seems like it's not vuln to RFD

Kavalli † - June 17, 2013, 2:33 pm

(Jun 17, 2013 02:01 PM)PacketMaster Wrote: [\[CITE\]](#) Thanks for the vuln .gov!

but guess what, i dont give a shit! find a vulnerability in cisco and then i will be impressed!

Why the fuck would he try to impress YOU?

Pendragon - June 17, 2013, 2:34 pm

(Jun 17, 2013 02:11 PM)lordsql Wrote: [\[CITE\]](#) Wow this forum post turned into idiocy. .gov websites are not anything to be proud of on Hf these days nor do people get any props for finding them, so i just posted the vuln.

It isn't vulnerable, that's the problem.

(Jun 17, 2013 02:13 PM)Andrew Downsend Wrote: [\[CITE\]](#) Thanks for the vuln, exploited with no issues. Good job OP.

Lie.

(Jun 17, 2013 02:30 PM)The Fail Collective Wrote: [\[CITE\]](#) Are you sure? I mean... are you really sure?

Seems like it's not vuln to RFD

I hope you're trolling.

Flaaffy - June 17, 2013, 2:35 pm

".gov websites are not anything to be proud of on Hf these days nor do people get any props for finding them"

so if you know people get no props for finding them then why would you post it here, move on -.-

also @ versace , did I say he should impress me? no i said, then i would be impressed. dont be such a mentresual dick

The Fail Collective - June 17, 2013, 2:37 pm

(Jun 17, 2013 02:34 PM)Pendragon Wrote: [\[CITE\]](#) I hope you're trolling.
What do you mean you hope I'm trolling?

Becky G - June 17, 2013, 2:41 pm

@Packet, i was just giving a freebie, not sure why everyone started flaming. And my title was of a joking matter if that's what it's over.

Pendragon - June 17, 2013, 3:00 pm

If you say that this is actually vulnerable, and extremely easy to exploit, why not provide a PoC to prove us all wrong? Something like this would suffice: <http://turf.unl.edu/CFIDE/skad.txt>

Becky G - June 17, 2013, 3:05 pm

Nice, I've been trying to find a good tutorial on CF9, can't find one.

amus3d - June 17, 2013, 4:26 pm

(Jun 17, 2013 01:53 PM)MiRP_Anon Wrote: [\[CITE\]](#) You found a login page? Congrats /sarcasm
yes, a login page that is, well running a patched version but unpatched is obvs, vuln to an old exploit - it shows it is CF v8 aka one of the vuln versions.

(Jun 17, 2013 01:57 PM)Vitanis Mate Wrote: [\[CITE\]](#) Then do it? It's not impressive unless you actually exploit it.
it still wouldnt be impressive even if he exploited it.

(Jun 17, 2013 02:01 PM)PacketMaster Wrote: [\[CITE\]](#) Thanks for the vuln .gov!
okay. have an unrefined google dork for a lot of gov's that run CF either patched or already hacked by kids, like yourself:
inurl:.gov ext:cfm

(Jun 17, 2013 03:05 PM)lordsql Wrote: [\[CITE\]](#) Nice, I've been trying to find a good tutorial on CF9, can't find one.
Odayz.

big hecks, no whammies,
amus3d.

Becky G - June 17, 2013, 5:04 pm

Amus3d sums it up once again. u da best.
congratz on 3,333 posts.

Sylvester - June 17, 2013, 9:11 pm

A. fucking. Mazing!! You found a god damn motha fucking Admin login page -.- Woow.

Flaaffy - June 17, 2013, 11:23 pm

(Jun 17, 2013 04:26 PM)amus3d Wrote: [\[CITE\]](#) yes, a login page that is, well running a patched version but unpatched is obvs, vuln to an old exploit - it shows it is CF v8 aka one of the vuln versions.

it still wouldnt be impressive even if he exploited it.

okay. have an unrefined google dork for a lot of govs that run CF either patched or already hacked by kids, like yourself:

inurl:.gov ext:cfm

Odayz.

big hecks, no whammies,
amus3d.

Mmm becuase in my post I blatantly said that in a non sarcastic tone, quote the rest of my post asshole. I don't even hack that much nowadays, to busy