Quassel IRC - Bug #366

CTCP PING handler potentially dangerous

10/24/2008 10:32 AM - Sputnick

Status:	Resolved	**Start date:**	
Priority:	Immediate	**Due date:**	
Assignee:	EgS	**% Done:**	0%
Category:	Quassel Core	**Estimated time:**	0.00 hour
Target version:	0.3.1		
Version:	0.13.1	**OS:**	Any

Description

[09:41:05] <coekie> looks like you've got a bug that allows an attacker to let you unwillingly send his irc commands to the server
[09:41:39] <Sput> oh?
[09:42:04] <Sput> how would that happen?
[09:42:42] <coekie> a ctcp PING sends back what it received, but **after** converting encoded newlines (and doesn't encode them when sending)
[09:43:35] <Sput> oh, so somebody could encode commands in the ping's payload
[09:43:38] <coekie> for example, if I would say: \001PING \020nPRIVMSG #quassel :hello
[09:43:47] <coekie> then you would send hello to #quassel :)
[09:43:59] <Sput> that is interesting indeed
[09:44:13] <Sput> sometimes such issues lurk where you expect them the least :)
[09:44:49] <coekie> ... \001PING \020nPRIVMSG Chanserv op #quassel\020nMODE #quassel +o coekie ... you get the point ;)

History

#1 - 10/25/2008 05:21 PM - Sputnick

http://git.quassel-irc.org/?p=quassel.git;a=commit;h=bcc567f2559058f38ca8ffecf7ef4428483cb540