ET: Legacy Development - Bug #1236

Check for malformed IP breaks IPv6

31.03.2019 11:03 - lefo

Status:	New	**% Done:**	0%
Priority:	Normal	**Spent time:**	0.00 hour
Assignee:			
Category:	Mod generic		
Target version:	2.78		
OS:		**Arch:**	

Description

Unlike other fields in userinfo ip is set by server.
If client attempts to inject some forged ip it gets replaced by server.
However this can still be tricked by injecting two or more ip fields.
In that case first injected ip gets removed server ip is appened and second injected ip gets used.

That's why it is necessary to check whether there is no more than one ip field.
Nevertheless when there is only one ip field we can be sure that it's the one provied by server so this field can be trusted and there is no need to check it for integrity.

For now this check only breaks IPv6 and is not otherwise any useful.
So let's just get rid of it.

–

Note that current checks for repeated field in userinfo are buggy.
For example clients with name ip get banned.

Check for injected ip fields and other syntax checks (such as odd slashes) should be probably done in sv_client.c instead.

Checks for other repeated fields in g_client.c seems hacky. These should be probably rewritten to use Info_NextPair or dropped entirely.

History

#1 - 31.03.2019 12:45 - Spyhawk

- Target version set to 2.78

Note: IPv6 support is currently disabled by default.

#2 - 31.03.2019 13:09 - lefo

Yeah, I think that's a bad thing. Let's enable it by default. I have game compiled with IPv6 enabled and it seems to be working just fine. Well, except for this issue.

Spyhawk wrote:

> Note: IPv6 support is currently disabled by default.

Files

0001-game-Remove-check-for-malformed-IP-in-userinfo.patch	2.88 KB	31.03.2019	lefo