Revision 1

EXPLOITING STEAM LOBBIES AND MATCHMAKING

BY LUIGI AURIEMMA

Description of the security vulnerabilities that affected the Steam lobbies and all the games using the Steam Matchmaking functionalities.

TABLE OF CONTENTS

Contents

Introduction 1

Steam lobbies and security risks 2

Description of the issues 4

The proof-of-concept 7

FAQ 8

History 9

Company Information 10

INTRODUCTION

Introduction

STEAM

"Steam[1] is an internet-based digital distribution, digital rights management, multiplayer, and communications platform developed by Valve Corporation. It is used to distribute games and related media from small, independent developers and larger software houses online."[2]

It's not easy to define Steam because it's not just a platform for buying games but also a social network, a market for game items, a framework[3] for integrating various functionalities in games, an anti-cheat, a cloud and more.

But the most important and attractive feature, from a security point of view, is its incredible diffusion[4] [5].

MATCHMAKING AND LOBBIES

Steam offers a simple and efficient way to allow games to provide online multiplayer functionalities to their users by using Steam Matchmaking.

Steam Matchmaking can be compared to a chat server where any user can create his own room (the “lobby”) that will appear in a public online list and other players can join it.

It’s possible to configure the lobby in various ways, for example adding custom parameters like name and game data, maximum number of joinable players, making it non-joinable or private or for friends only, sending chat messages, running a game server and more.

The interaction with this matchmaking system is granted by the set of Steamworks APIs contained in the IsteamMatchmaking class, so any game can use this feature.

Many games use the Steam lobbies for online gaming: Counter Strike Global Offensive, Left for Dead 1 and 2, Borderlands 2, Payday 2, the Codemasters games (Dirt, Grid and F1 series) and **any** multiplayer game sold on Steam that is not based on the Source engine or proprietary solutions.

Steam Matchmaking gained some notoriety in the last years due to the “migration” performed by the developers/publishers of many games from a master server architecture, private or hosted by Gamespy, to the Steam one. This solution granted some of them to survive from the Gamespy shutdown of May 2014[6].

[1] http://steampowered.com
[2] http://en.wikipedia.org/wiki/Steam_(software)
[3] http://www.steampowered.com/steamworks/
[4] http://www.joystiq.com/2014/01/15/steam-has-75-million-active-users-valve-announces-at-dev-days/
[5] http://www.dualshockers.com/2014/06/29/steam-passes-8-million-concurrent-users/
[6] http://www.wired.com/2014/06/gamespy-server-shutdown/

STEAM LOBBIES AND SECURITY RISKS

Steam lobbies and security risks

HOW THE STEAM LOBBIES WORK

In technical terms the concept of the Steam lobbies is quite simple:

- An user starts a lobby (CreateLobby)
- He sets some lobby parameters (SetLobbyData)
- The other users can view the new lobby when they query the list of public lobbies (GetLobbyByIndex)
- The users join the lobby (JoinLobby)
- At this point joining the game server (which is separate from the Steam lobby) is game dependent, some games use SetLobbyGameServer, others get the lobby owner's SteamID (GetLobbyOwner), others put that ID in a lobby parameter, others specify the IP and port of the server instead of the SteamID and so on
- When the clients have the owner's ID, they can join his game server using the Steam Networking API (SendP2Ppacket)

What is visualized in-game to the players is not different than any other "master server"-based game, additionally Steam automatically sorts the lobbies based on the geographic distance between the lobby's owner and the user who requested the list to allow the quick-matchmaking feature (auto-joining servers with best ping and maybe with players of same nationality).

SECURITY TESTING AND EFFECTS

The vulnerabilities in the Steam Matchmaking have been found during a research commissioned by Epic Games[7] regarding the third-party libraries and services used in their Unreal Engine 4[8].

The tests have been started the 25th July 2014.

Some issues were discovered with the following security effects:

- Takeover of the lobby owned by other users
- Forcing all the players in a lobby to leave it and joining an inexistent game server
- Setting custom parameters of any lobby
- Making any lobby not publicly visible
- Performing these operations without even joining the lobby

[7] http://epicgames.com

[8] http://www.unrealengine.com

STEAM LOBBIES AND SECURITY RISKS

The main effect of these vulnerabilities, affecting the Steam back-end network, is that an attacker can deny the online gaming of several known and played multiplayer games with a simple and silent attack performed in a couple of seconds.

VULNERABLE VERSIONS

The Steam back-end network that handles the lobbies was vulnerable till the 17th September 2014.

NON-VULNERABLE VERSIONS

Currently all the reported issues have been fixed.

An undefined number of old games has been left vulnerable ("whitelisted") due to how they implement the Steam Matchmaking, probably because their P2P oriented gaming requires that any user can act as co-owner of the lobby. For these games may be released game-related patches in future if necessary.

No further details are available.

DESCRIPTION OF THE ISSUES

Description of the issues

SETLOBBYGAMESERVER DENIAL OF SERVICE

Joining a game server, after having joined a lobby, is a game-dependent operation.

Steamworks in its SpaceWar example game, used to show to the game developers how to implement the Steamworks API, suggests to use the SetLobbyGameServer API and automatically joining the server upon the execution of a specific callback.

When that API is executed Steam sends an event to all the users in the target lobby that will execute the LobbyGameCreated_t callback and adds the following lobby parameters:

- __gameserverIP – IP address of the game server or 0
- __gameserverPort – port of the game server or 0
- __gameserverSteamID – SteamID of the user running the server or 0

Valve suggests that the default behavior is leaving the lobby and connecting to the game server:

```
//-----------------------------------------------------------------------------
// Purpose: A game created a game for all the members of the lobby to join,
//          as triggered by a SetLobbyGameServer()
//          it's up to the individual clients to take action on this; the usual
//          game behavior is to leave the lobby and connect to the specified game server
//-----------------------------------------------------------------------------
struct LobbyGameCreated_t
{
    enum { k_iCallback = k_iSteamMatchmakingCallbacks + 9 };

    uint64 m_ulSteamIDLobby;         // the lobby we were in
    uint64 m_ulSteamIDGameServer;    // the new game server that has been created or found for
                                     // the lobby members
    uint32 m_unIP;                   // IP & Port of the game server (if any)
    uint16 m_usPort;
};
```

That's the default behavior that happens with SpaceWar, AlienSwarm, Borderlands 2 and some other games.

That API can be called not only by the owner of the lobby but also by any other user that joins that lobby, this is the reason why this feature can be abused to force the other players to leave the lobby trying to join an arbitrary IP or SteamID.

Performing this operation against all the available lobbies of an affected game, will result in the absence of online lobbies and in clients that try to connect to inexistent servers. In some games like Alien Swarm there are no visible effects for the owner of the lobby and other players, they will silently leave the lobby (that will be automatically deleted when left by the owner) but nothing is shown to the players.

DESCRIPTION OF THE ISSUES

TAKEOVER OF STEAM LOBBIES

Steamworks provides various ways to the users for controlling and customizing their lobbies:

- SetLobbyData and DeleteLobbyData
  Adds, modifies and deletes the lobby parameters, for example “name”
- SetLobbyMemberLimit
  Limits the amount of users who can join the lobby
- SetLobbyType
  Allows to set the lobby as:
  - Private: invisible to the public list and to the friends
  - FriendsOnly: invisible to the public list, but visible to the friends
  - Public: default
  - Invisible: allows an user to join two lobbies
- SetLobbyJoinable
  Allows to make the lobby non-joinable
- SetLobbyGameServer
  The API seen before

The following are some real examples of Steam lobbies taken from Borderlands 2, F1 2013, XCom-Enemy-Unknown and Payday 2, they are useful to understand better what are the lobby parameters:

```
lobby 109775241376664452 - 459508612 393216 8 1
  BuildUniqueString: BORDERLANDS2-1.8.3W
  CurrMission: 7
  CurrPlotMission: 7
  DlcFlag: 1
  DlcMapContentId: 0
  DlcMapPackageId: 0
  gameMode: 0
  HostExpLevel: 31
  IsPublic: 1
  OwningPlayerName: TRUCKERBOX
  PlayThrough: 1
  __gameserverIP: 0
  __gameserverPort: 0
  __gameserverSteamID: 765611981062*****
```

```
lobby 109775241376111944 - 458956104 393216 8 1
  268435458: 65365
  536870936: 0
  SteamLobbyGameMode: 0
  SteamLobbyGameType: 0
  SteamLobbyHostId: 765611980157*****
  SteamLobbyHostName: ICEMAN
  SteamLobbyOpenSlots: 15
  SteamLobbyVisibility: 0
```

```
lobby 109775241373641018 - 456485178 393216 8 1
  268435468: 0
  268435469: 0
  268435470: 90
  268435471: 10000
  268435472: 0
  268435474: 0
  268435488: 1724
  268435489: 28398179
  32779: 0
  553648128: 9212610293214#24968160127#
  bIsDedicated: False
  BotPlayerCount: 0
  bUsesStats: True
  GameSettings: XComOnlineGameSettingsDeathmatchRanked
  GameTags: XComMPLobbyGame
  MapName: XComShell
  MaxPlayerCount: 1
  NumOpenPrivateConnections: 0
  NumOpenPublicConnections: 1
  NumPrivateConnections: 0
  NumPublicConnections: 2
  OwningPlayerId: 765611980191*****
  OwningPlayerName: Kharon
  PasswordProtected: 0
  ServerName: Kharon
  SteamEngineVersion: 8916
  __gameserverIP: 0
  __gameserverPort: 0
  __gameserverSteamID: 900914655904*****
```

```
lobby 109775241376713535 - 459557695 393216 8 1
  difficulty: 5
  drop_in: 1
  job_class_max: 80
  job_class_min: 80
  job_id: 28
  kicking_allowed: 1
  level: 57
  lobby_type: public
  min_level: 0
  num_players: 1
  owner_id: 765611980432*****
  owner_name: rendoman
  payday2_v1.12.4: true
  permission: 1
  state: 3
  __gameserverIP: 0
  __gameserverPort: 0
  __gameserverSteamID: 765611980432*****
```

These APIs can be called by any user, not only the lobby owner and, moreover, they can use used even from outside the lobby. That means an attacker is able to silently delete any online lobby without even joining them and resulting in a multiplayer game without online matches to join.

THE PROOF-OF-CONCEPT

The proof-of-concept

A proof-of-concept is available as reference for the issues:

- http://revuln.com/files/steam_lobby_poc.cpp

Please note that the issues have been fixed and that proof-of-concept no longer works, except for the whitelisted games.

FAQ

What was the impact of these issues?

A single attacker, without particular network or bandwidth requirements, was able to make many multiplayer games unplayable online with zero lobbies/matches to which connecting. The attack was silent and performed in some seconds without even joining the target lobbies.

Were these issues critical?

Yes, without Steam lobbies it's not possible to play online with many multiplayer games sold on Steam.

Are these issues fixed now?

Yes, all the issues have been definitely fixed the 17th September 2014.

Some old games have been left whitelisted by Valve due to backward compatibility (basically their multiplayer has been designed to work in that way) and so they may be still vulnerable "by design".

Was the attack performed against the users' computers?

No, the Steam lobbies are handled by the Steam back-end network.

Does the attacker need to own the target games to attack them?

It depends by the game, retrieving the list of online lobbies is an operation usually available to who owns the game but some games can be queried even from accounts that don't own them.

Was/is the game X vulnerable?

There is a short list of some tested games in the Introduction section.

If you want to know if a game uses the Steam lobbies you can use some tools[9], while if you are interested to test it you can use the proof-of-concept provided in the previous section of this paper.

[9] http://aluigi.org/papers.htm#steamlobbylist

HISTORY

History

- `25 Jul 2014` Security issues initially found
- `04 Aug 2014` Vulnerabilities reported to Valve after more tests on various games
- `12 Aug 2014` The APIs can be no longer called from outside the lobbies without joining
- `23 Aug 2014` Some mitigations implemented by Valve, still possible to make lobbies private
- `17 Sep 2014` After many e-mails all the remaining issues have been fixed, only the owners of the lobbies can perform operations on them

COMPANY INFORMATION

Company Information

ReVuln Ltd.
Level 3, Theuma House, 302, St.Paul Street,
Valletta VLT1213
Malta

http://revuln.com
@revuln
info@revuln.com