


master ▾

1 branch

0 tags

Go to file

Code ▾

 sammwyy Merge pull request #1 from MacacoLew/patch-1 ...

a8981c6 on Feb 9

26 commits

README.md

Fix a typo

4 months ago

README.md

# Advanced Server Security Guide

An advanced guide for protect your minecraft server or network.

## Index

- 1. Introduction
  - What is this guide for?
  - Why do I need to secure my server?
  - What I need?
  - Disclaimer
- 2. Bungeecord
  - Default configuration
  - Authentication plugin
  - What plugins should i not use
  - Block Invalid Packets
  - Block Exploits
  - Block Bots
  - World Downloader
  - Block Commands
  - Host Limiter
  - Premium Mode
  - Bungee Authme
  - Hide Plugins
  - Summary
- 3. Spigot
  - Block Spigot Exploits
  - Block OP
  - IP Based Protection
  - Cracked Authentication
  - WorldEdit Crash
  - For Creative Servers
  - Block Items Duplication
  - KickAll Exploit
  - UUID Spoof
  - Custom Payload Exploit
  - Bot Protection for Spigot
  - Hide Plugins in Spigot
  - 2nd Check for Staff
  - IPWhitelist
  - Book Exploit
  - Bad Potion Exploit
  - Skull Exploit
  - Spigot Summary
- 4. Extra
  - Firewall
  - IP Forward
  - Hide spigot ports

About

An advanced guide for protect your minecraft server or network.

[arkflame.com](#)

Readme


Releases


No releases published

Packages

No packages published

Contributors 2

 sammwyy Sammwy

 LewUwU

# Introduction

## 🔗 Introduction

### 🔗 What is this guide for?

This guide is created with the sole purpose of protecting our server against exploit abuse that could damage the server or network.

With this guide you can block most exploits and bugs that the Grieffers (A.K.A Skiddies) use to break our cubes.

### 🔗 Why do I need to secure my server?

If you search on Google "Grief minecraft server" this will give you enough reason to protect your server, in summary you run the risk that your account is compromised or that hacked clients can attack your vulnerable minecraft server/network.

### 🔗 What I need?

You don't need much knowledge, try to know at least: how plugins are installed, how they are configured, how ports work, how servers and packets work. Also to improve security I recommend not using host pages, use a VPS or Dedicated (Best option)

### 🔗 Disclaimer

It is impossible to block all exploits, most of the grief is due to the stupidity of the owners, administrators or who has made a patent configuration of the server as the fact of using plugins with bypasses or configuring them incorrectly. Nor do I promise you that your network/server will be completely inescapable, nor will I be responsible for any damage you do to your server with this guide. (If you follow everything to the letter nothing bad will happen)

# Bungeecord

## 🔗 Bungeecord

If you don't use bungeecord (which one you should use) you can skip this part even though I don't recommend it at all.

### 🔗 Default configuration

The bungeecord server already comes with a default configuration that helps users understand how it works, but it is dangerous to leave some parameters as they are.

```
# Leaving this is quite dangerous.
groups:
  md_5:
    - admin

# change them to how they are continuing
groups:
  md_5: []

# make sure that the following values are as follows.
ip_forward: true
prevent_proxy_connections: true

# This only if your server has support for non-premium users or if you want users to enter the lobby
listeners:
  force_default_server: true
```

### 🔗 Authentication plugin

Never use auth plugins in the bungeecord, it may sound safe but it can be exploited in many ways, it is best to have a dedicated auth server, in case of using multiple lobbies use a MySQL connection. Also do not use AuthmeBridgeBungee and if you are not going to listen to this point and you will still place an Auth plugin in the bungee, at least use [DynamicBungeeAuth](#) that of all of the market, is the one that is best programmed in my opinion.

Example of exploit: if you are kicked from the spigot instance but the bungeecord does not eject your currentServer variable it could be null giving you the opportunity to bypass functions locked on the auth server. As an example changepassword or unregister (It happens when you send packets to the spigot server that this closes your connection instantly in an insecure way which the bungeecord fails to detect)

### 🔗 What plugins should i not use

It is advisable to have the minimum possible plugins in the Bungeecord instance, even so avoid placing this type of plugins:

1. Global report system (Like any "/report" plugin)
2. Global moderation system (Like Litebans)
3. Global message system or staff chat

4. Permissions plugins for bungeecord (Like BungeePerms)
5. Any authentication plugin (Like BungeeAuth)
6. Viaversion (Use Flamecord or Travertine)
7. Any antivpn/proxy system.

### 🔗 Block Invalid Packets

To protect our server from attacks of invalid exploits and packages, it is advisable to use Flamecord (Flamecord is a proxy software, travertine fork that mitigates exploit attacks) [download it here](#).

### 🔗 Block exploits

we can secure our spigot servers from the bungeecord instance with some useful plugins, [ExploitFixer](#) is the most recommended (and it's free)

### 🔗 Block bots

The most advisable thing is to block bots in the instance bungeecord, for this we will use the following [Antibot plugin](#).

Remember that bot attacks cause a waste of resources on your server that can crash it.

### 🔗 World Downloader

To prevent users from downloading our server constructions using WorldDownloaderMod, we will use this [plugin](#) that blocks that mod.

### 🔗 Block Commands

Here is a way to block global commands on our server, this can be very useful to disable commands that can compromise server security.

for this we will use a plugin called [BungeeCommandBlock](#)

### 🔗 Host Limiter

Although it is not very useful but it can be if you put it to good use, you can block from which domain each user must enter or allow only 1 for all. Those who open the door to create a domain system for each staff on the server.

for this we will use a plugin called [BungeeHostLimiter](#)

### 🔗 Premium mode

It is not recommended since there have been cases of servers which this plugin has been bypassed but in the networks that I saw that they had it, these cases were not reported, and although it is not recommended if you had to choose a plugin in a premium way, I would choose [FastLogin](#)

### 🔗 Bungee Authme

Not to be confused with BungeeAuthmeBridge (this plugin is garbage), the following plugin is official from Authme developers and simply blocks the actions sent to the bungee by users who have not logged in. (Commands, messages, etc.)

Warning: It could cause incompatibility with premium authentication plugins.

Plugin: [AuthmeBungee](#)

### 🔗 Hide Plugins

To prevent users from observing the server plugins using the TabComplete method, we can use the plugin called: [CanelaAntiPluginSteal] (<https://www.spigotmc.org/resources/canela-anti-pluginsteal.1150/>)

### 🔗 Summary

The truth is not necessary to follow all these steps except for [Block Bots](#), [Block Exploits](#) and [Block Invalid Packets](#). While everything is in order it should not be why there are exploits in the bungeecord.



### 🔗 Spigot

### 🔗 Block Spigot Exploits

As in bungee, we must protect our Spigot server from exploit attacks, for this we will use this plugin. [Exploitfixer](#) works for both Spigot and bungeecord, it is advisable to have it in both instances since there are exploits for spigot that bungee is unable to detect.

### 🔗 Block OP

It is highly recommended to block the OP and not give it to anyone, not even have it ourselves. To block that a user can obtain OP thanks to a permit or by another operator, we will use [Anti ForceOP](#).

You can also configure that operators do not have any type of permissions by changing this parameter in the spigot server configuration:

```
op-permission-level=0
```

Default value: 4

Recommended value: 0

## 🔗 IP Based Protection

If you want one more layer of protection, you can protect the accounts of all staff using [AccountGuard](#). This plugin allows you to restrict the IP address from which you can access an account. In this way you can protect your account or those of the staff so that they can only be accessed from their respective IP address.

## 🔗 Cracked Authentication

If your server supports non-premium players, you must have an authentication plugin, otherwise your server will be compromised to hacked clients. For this you can use a plugin below:

[Authme Reloaded](#) (Recommended).

[Login Security](#).

## 🔗 WorldEdit Crash

There are several exploits when using worldedit that can crash the server besides that this plugin uses many resources and its tasks are Sync (that is, that the users will suffer from lag and the server will be frozen while this plugin is working) to correct this we will use [FastAsyncWorldEdit](#)

## 🔗 For Creative Servers

There are several hacked clients capable of generating malicious, corrupt items or with custom NBT tags that can range from crashing to the server to taking huge enchantments.

For this we will use [ExploitFixer](#) and/or [ItemFixer](#).

## 🔗 Block Items Duplication

By default the minecraft code has some bugs that allow duplicate objects in the chests taking advantage of certain bugs, to solve this you can use a plugin below:

[ExploitFixer](#) (Recommended).

[Dupe Fixes](#) (Dedicated plugins just for Dupe Exploits).

[Confiscate](#) (Premium and excellent option with some usefull functions!!)

## 🔗 KickAll Exploit

Normally in minecraft when you enter the server and your account is already online, it is disconnected giving way to the most recent connection, authme and bungeecord solve this but if your server is a network and you choose to use ipwhitelist since you can not install a software firewall then your server is vulnerable to an exploit that matches for each online player, making a connection which kicks the selected player (kicking all players)

To solve this we will use the plugin called [AntiUserSteal](#)

## 🔗 UUID Spoof

Hacked clients can easily change their uuid, which imposes a great risk for servers without adequate protection, luckily there are several plugins that solve this, for example [ExploitFixer](#) and [AntiUUIDSpoof](#) (Recommended for mixed-mode).

## 🔗 Custom Payload Exploit

CustomPayload packets are called packages that are sent to the server with a specific parameter, these packages are mostly used for communication between the client and the server in some mods or for communication between spigot/bungeecord.

Sending such large-scale packets or packets that the server cannot process can crash the server if it does not have adequate protection.

To solve this we can use [ExploitFixer](#) or [CustomPayloadFixer](#).

## 🔗 Bot Protection for Spigot

If you do not have a bungeecord instance then the plugin mentioned in [Block bots](#) will not work for you, here is a list of antibot plugins which could be useful:

[AntiBot-Ultra](#).

[AntiBot-Attack](#).

Remember that bot attacks cause a waste of resources on your server that can crash it.

## 🔗 Hide Plugins in Spigot

If you do not have a bungeecord instance then the plugin mentioned in [Hide Plugins](#) will not work for you, to block users from seeing your plugins you can use [PLSecure](#),

## 🔗 2nd Check for Staff

If you want to have a second authentication for your administrative staff then you can opt for this plugin.

[PinProtect](#) adds a second authentication in the form of a pin in case the password is bypassed. (It is advisable to place it in the lobby)

## 🔗 IPWhitelist

It is highly recommended that you have a firewall software on the server system, but if you do not have access to a terminal either because you use a web page that offers a host for minecraft servers or for any other reason and you have a Network, then you must use [IPWhitelist](#).

[IPWhitelist](#) restricts from which bungeecord your Spigot server can be accessed. otherwise the door is open to which they can access with any username if they discover the port of your Spigot server.

## 🔗 Book Exploit

There are hacked clients able to create books with almost infinite enchantments. These books when interacting with a user cause the server to have to process a lot of information causing a memory overflow and causing it to close.

To fix this we can use [Book-Sign Exploit Fix](#) or [ExploitFixer](#).

## 🔗 Bad Potion Exploit

as well as hacked books, the same thing happens with potions, [AntiHackedPotions](#) or [ExploitFixer](#), those plugins detects potions with dangerously high spells or that can get the server crashed and removes them.

## 🔗 Skull Exploit

Like the previous points, minecraft heads have many properties that can be exploited and corrupt worlds, chunks or crash the server. We can detect and remove them using [Skull Exploit Fix](#) or [ExploitFixer](#).

## 🔗 Spigot Summary

the truth is that most exploits are covered by [ExploitFixer](#), but do not overlook AntiBot protection and some points that [ExploitFixer](#) still does not solve.



## 🔗 Extra

### 🔗 Hide spigot port

The most advisable thing is to use a firewall to block the ports of the spigot servers from ips that do not come from the local network (127.0.0.1) but making spigot only listen to the local IP (127.0.0.1) is a good practice that NEVER forget.

```
# On spigot servers (server.properties)
server-ip= 127.0.0.1
```

```
# On bungeecord instance (config.yml)
# in any server in the "servers" list:
servers:
  server-1:
    address: 127.0.0.1:xxxxx
    restricted: false
  server-2:
    address: 127.0.0.1:xxxxx
    restricted: false
  server-3:
    address: 127.0.0.1:xxxxx
    restricted: false
```

## 🔗 IP Forward

if the bungeecord hook or ip forward are deactivated then the spigot servers will be unable to recognize the IP address of the users.

For this we will place the `ip_forward` option in the bungeecord config.yml to true, and the "bungeecord" option in the spigot.yml file of all spigot servers to true.

```
# Config.yml of Bungeecord
ip_forward: true
```

```
# Spigot.yml of each spigot server
settings:
```

bungeecord: [true](#)

## 🔗 Firewall

A firewall is a software that allows us to restrict incoming and outgoing connections to the server, it is extremely recommended to use [IPTables](#) or [UFW](#).

You can get more information searching on the internet.

## 🔗 The END

🔗 Made with ❤️ Need help? contact me on discord (view my github profile) or contact me on twitter: [@Sammwy\\_](#)

