Below, are details of preventative measures you can take in order to prevent malicious players from taking control of, or 'crashing' your Wolfenstein: Enemy Territory game server. Some are version specific, others are not.

Quake 3 Download Exploit - Versions vulnerable: 2.55, 2.56, 2.60

The Exploit

A bug in the Q3 engine allows a malicious player to download any file from the server, providing they know the file name. As an example, the malicious player will attempt to download 'server.cfg', which contains your RCON and referee passwords. These can then be used to take full control over your server.

Preventative Measures

There are several ways to prevent a malicious player from gaining access to your server's passwords via this method:

1. Disable downloads: Disabling downloads will prevent the malicious player from using the exploit, thus preventing the passwords being obtained.

2. Rename server.cfg: Renaming your server.cfg to something unguessable (such as oaskldj239U8SDHKA89uekl.cfg) will prevent the malicious player from being able to download your configuration files and passwords.*

3. Set RCON password in start-up line: By setting your server's RCON password in the start-up line, your server's configuration file will no longer need to contain your server's password.

* Note that other files on your server may contain your rcon password (such as configuration files for etadmin_mod). These should also be renamed for maximum security.

Quake 3 Engine 'Oversize Infostring' exploit - Versions vulnerable: 2.55, 2.56, 2.60

The Exploit

A malicious player can shut down or crash a game server, as the Q3 engine has problems handling large queries. If your server is attacked via this method, the following will be present in your console log file:

ERROR: Info_SetValueForKey: oversize infostring

Preventative Measures

Fortunately, it is possible to completely prevent this issue from occuring by patching the server's etded.x86 (Linux) or etded.exe (Windows). A patch (q3infofix.zip) is attached to the end of this post.**

** Your server host may already have applied this fix. If not, most hosts will be willing to do this for you.

/callvote Exploit - Versions vulnerable: 2.55, 2.56, 2.60, 2.60b

The Exploit

The exploit allows a malicious user to execute any command via the /callvote command. The vote must pass for the command to be executed.

Preventative Measures

There are several ways to prevent this exploit from being used on your server:

1. Disable voting: The simple solution is to disable voting. If a vote cannot be called and passed, commands cannot be executed via this method.

2. Use the latest mod version: Several mod developers are integrating fixes into their mods (ETPub 0.9.0 nightly includes this fix). Check the mod developer's web sites / change logs to see if the exploit it patched.

For ETPro, the combinedfixes.lua module patches the exploit and is attached to this post (combinedfixes.zip).

Fake Players DOS Attack - Versions vulnerable: 2.55, 2.56, 2.60, 2.60b

The Exploit

A malicious player can fill a server with 'fake' players. This prevents 'real' players from being able to join.

Preventative Measures

1.Mods preventing the exploit: Some mods (generally later versions) include fixes such as limiting the number of connections from a single IP address. Later ETPub versions include this. Check the mod websites / change logs to see if the exploit is fixed.

2.ETPro LUA module: For ETPro only, the combinedfixes LUA module prevents the fake players DOS attack. The combinedfixes LUA module is attached to this post (combinedfixes.zip).

/ws Exploit - ETPRO ONLY! - Versions vulnerable: 2.55, 2.56, 2.60, 2.60b

The Exploit

The /ws command in the ETPro mod can be used to crash servers and / or obtain information such as server passwords.

Preventative Measures

Running the combinedfixes lua module prevents this exploit. The lua module is attached to this post (combinedfixes.zip).

etadmin_mod Exploits - ETADMIN_MOD ONLY! - Versions vulnerable: 2.55, 2.56, 2.60, 2.60b

The Exploit

Certain names will allow malicious players to gain administrator control over your server via etadmin_mod.

Preventative Measures

Find the following in bin/etadmin_mod.pl:

```
elsif ( index( $line, "Userinfo" ) == 0 )
    {

        #$line =~ /cl_guid\\([^\\]*)\\.*name\\([^\\]*)\\.*\\/; #ip\\(\d+\.\d+\.\d+\.\d+):\+\\/;
        my $rhash          = &parse_userinfo($line);
        my $guid           = $$rhash{'cl_guid'};
        my $name           = &strip_name( $$rhash{'name'} );
        my $ip             = $$rhash{'ip'};
        my $custom_password = $$rhash{'hp_password'};
        my $custom_exec     = $$rhash{'hp_logincmd'};
        my $greeting        = $$rhash{'hp_greeting'};

        $kick = "";
        $ip =~ s/:.*$//;

        $over_ip      = $ip;
        $over_guid    = $guid;
        $over_name    = $name;
        $ready{$guid} = time;
```

Replace it with:

```
elsif ( index( $line, "Userinfo" ) == 0 )
    {

        #$line =~ /cl_guid\\([^\\]*)\\.*name\\([^\\]*)\\.*\\/; #ip\\(\d+\.\d+\.\d+\.\d+):\+\\/;
        my $rhash          = &parse_userinfo($line);
        my $guid           = $$rhash{'cl_guid'};
        my $name           = &strip_name( $$rhash{'name'} );
        my $ip             = $$rhash{'ip'};
        my $custom_password = $$rhash{'hp_password'};
        my $custom_exec     = $$rhash{'hp_logincmd'};
        my $greeting        = $$rhash{'hp_greeting'};

        $kick = "";
        $ip =~ s/:.*$//;
```

```
        # START: Lucel's admin steal fix....
    if ( $$rhash{'name'} =~ /.+\^$/ )
    {
      &log("Kicked $name. Has trailing carrot in their name, can be used to hack etadmin mod!");
      $kick = "You have an invalid name! Please remove the last character!";
      next;
    }
        # END: Lucel's admin steal fix....

        $over_ip      = $ip;
        $over_guid    = $guid;
        $over_name    = $name;
        $ready{$guid} = time;
```

Credits:

Luigi Auriemma
/dev/humancontroller
ReyalP
SNL Lucel

Download: combinedfixes.zip(3.8 Kb) · q3infofix.zip(3.7 Kb)