

[UNIX] Eggdrop Bot Share.mod Vulnerability Can Lead To Takeover

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-02/0027.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 02/11/04

To: list@securiteam.com

Date: 11 Feb 2004 16:47:06 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Eggdrop Bot Share.mod Vulnerability Can Lead To Takeover

SUMMARY

" <<http://www.eggheads.org/>> Eggdrop is the world's most popular Open Source IRC bot, designed for flexibility and ease of use, and is freely distributable under the GNU General Public License (GPL)."

A vulnerability has been discovered in the share.mod module provided with eggdrop source code. An attacker can gain control over (almost) any eggdrop botnet. The bug relies on the fact that every legitimate bot can gain share status even if it's not set to share with anyone.

DETAILS

Vulnerable Systems:

* Eggdrop version 1.6.15, possibly prior

The share.mod module uses tandem buffers to handle user file resync transfers. Tandem buffers are checked minutely by check_expired_tbufs() in order to flush tandem buffers older than 15 minutes (resync_time). The function check_expired_tbufs() also handles userfile requests in limbo (that haven't received any response from tandem bot). While doing those

Securiteam: [UNIX] Eggdrop Bot Share.mod Vulnerability Can Lead To Takeover

checks the programmer has left out some parentheses.

A snippet of code is shown below:

```
for (i = 0; i < dcc_total; i++)
  if (dcc[i].type->flags & DCT_BOT) {
    if (dcc[i].status & STAT_OFFERED) {
      if (now - dcc[i].timeval > 120) {
        if (dcc[i].user && (bot_flags(dcc[i].user) & BOT_AGGRESSIVE))
          dprintf(i, "s u\n");
        /* ^ send it again in case they missed it */
      }
      /* If it's a share bot that hasnt been sharing, ask again */
    } else if (!(dcc[i].status & STAT_SHARE)) {
      ----- /* Bug now every bot gain the STAT_OFFERED status. */
      if (dcc[i].user && (bot_flags(dcc[i].user) & BOT_AGGRESSIVE))
        dprintf(i, "s u\n");
      dcc[i].status |= STAT_OFFERED;
      ----- /* eof Bug */

    }
  }
```

As can be seen, every non-sharebot gains STAT_OFFERED status, minutely.

The next step is to gain STAT_SHARE, which can be obtained with share_ufyes(). That function doesn't STAT_SHARE check, just STAT_OFFERED:

```
static void share_ufyes(int idx, char *par)
{
  if (dcc[idx].status & STAT_OFFERED) {
    dcc[idx].status &= ~STAT_OFFERED;
    dcc[idx].status |= STAT_SHARE;
    dcc[idx].status |= STAT_SENDING;
    uf_features_parse(idx, par);
    start_sending_users(idx);
    putlog(LOG_BOTS, "*", "Sending user file send request to %s",
           dcc[idx].nick);
  }
}
```

And the bot is completely recognized as a sharebot and we can add a user, delete a user, etc. Two bots directly linked, at the moment of link, share a password (handshake) but two bots not directly linked probably won't. It is possible to fake a real bot by simply telneting to the bot port, writing the botnick, and pressing Enter.

Patch Availability:

An unofficial diff patch is presented below:

----- Cut Here -----

Securiteam: [UNIX] Eggdrop Bot Share.mod Vulnerability Can Lead To Takeover

```
--- eggdrop1.6.15/src/mod/share.mod/share.c Sat Feb 27 05:13:32 2004
+++ eggdrop1.6.15-sp/src/mod/share.mod/share.c ?Sat Feb 27 05:43:33 2004
@@ -1457,9 +1457,11 @@
    /* ^ send it again in case they missed it */
    /* If it's a share bot that hasnt been sharing, ask again */
    } else if (!(dcc[i].status & STAT_SHARE)) {
- if (dcc[i].user && (bot_flags(dcc[i].user) & BOT_AGGRESSIVE))
+ /* Patched from original source by giusc@gbss.it <20040207> */
+ if (dcc[i].user && (bot_flags(dcc[i].user) & BOT_AGGRESSIVE)) {
    dprintf(i, "s u\n");
- dcc[i].status |= STAT_OFFERED;
+ dcc[i].status |= STAT_OFFERED;
+ ?}
    }
  }
}
}
}
----- Cut Here -----
```

Vendor Status:

The vendor has been notified on February 7th, 2004.

ADDITIONAL INFORMATION

The information has been provided by <mailto:giusc@gbss.it> Giuseppe Caulo

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.