BSD Games

- **B391**: LINTING, Unsafe snprintf() Accumulation,
  FUNCTION: sail/sync.c:82
- **B509**: LINTING, Unsafe Function - atoi(),
  FUNCTION: robots/main.c:80,
  NOTE: Improper setgid privileges revocation prior
- **B218**: QUANDARY, SHELL INJECTION,
  FUNCTION: hack/hack.pager.c:429

ANGBAND

- **B1**: DEFAULT, NULL DEREF,
  FUNCTION: src/z-queue.c:24
- **B21**: **INFERBO**, INTEGER OVERFLOW,
  FUNCTION: src/z-rand.c:185
  NOTE: This might not be a bug but is interesting ...
- **B26**: **INFERBO**, BUFFER OVERRUN,
  FUNCTION: src/z-file.c:141
  NOTE: Shonky code - improper validation of the ```username``` string - lots of integer bugs
- **B42**: **INFERBO**, BUFFER OVERRUN,
  FUNCTION: src/obj-util.c:490
  NOTE: ```k == 120``` --> out by one buffer overwrite
- **B43**: DEFAULT, NULL DEREF,
  FUNCTION:src/target.c:228
  NOTE: ```mon``` can be NULL and is not checked
- **B52**: **INFERBO**, INTEGER OVERFLOW,
  FUNCTION: src/z-util.c:209
  NOTE: many examples - no range checking - also use of ```char`` rather than ```unsigned char```
- **B163**: QUANDARY,
  FUNCTION: src/main-x11.c:2318
  NOTE: Attacker controlled ENV passed to vulnerable function ```atoi```

SKYNET

- **B35**: **BUFFER OVERRUN**
  FUNCTION: lualib-src/lua-netpack.c:97
  NOTE: Portability bug or worse: use of signed rather than unsigned integers;
  Can be negative and/or overflow
- **B42**: DEAD STORE
  FUNCTION: lualib-src/lsha1.c
  NOTE: Crypto variables not deleted after use - compiler will eliminate assignment
- **B83**: **INFERBO**, INTEGER OVERFLOW
  FUNCTION: service-src/service_gate.c:190
  NOTE: Interesting cases because it looks like it's in protocol messaging so is security interesting
- **B134**: ARRAY SIZE IS ZERO,
  FUNCTION: lualib-src/lua-socket.c:448
  NOTE: The array size can't be dynamically assigned which appears to be the case here;