**Analysis Report: BusyBox ELF Binary**

**File Overview**

* **File Name**: chakravyuh.bin
* **File System**: Squashfs filesystem
* **File Type**: little endian

**Static Analysis**

**Cryptographic Analysis:** SHA,RSA,AES and private keys found. **Entropy :** ~8 **File Signature:** ELF,JPG,PNG,etc. **Firmware Details:** File Size: 22,106,176 bytes

MD5 Hash: 487471520fbaace46b1677890f4ef4c6

File Format: u-boot legacy uImage, hi3520Dromfs, Linux/ARM, OS Kernel Image (gzip), 13144064 bytes, Wed Nov 29 14:28:44 2017, Load Address: 0XA0060000, Entry Point: 0XA0DA0000, Header CRC: 0X71FF3C3D, Data CRC: 0X3F9F5075

Average Entropy: 7.81  
 **Potential Vulnerabilities**

**1. Hardcoded Credentials/Network Configurations:**

Observed:

IPs: 192.168.1.108, 192.168.1.1, etc.

Network-related fields: HOSTIP, SUBMASK, GATEWAYIP, BRIDGENAME.

Risks:

Hardcoded IPs and network details might indicate fixed defaults. If attackers know these, they could exploit the system by

targeting these default configurations.

**2. Insecure Function Usage:**

Functions Identified:

strcpy, sprintf, system.

Risks:

strcpy and sprintf are vulnerable to buffer overflow attacks.

system can lead to command injection if input is not sanitized.

**3. Log Error Messages:**

Observed:

Error logs with format strings (ERR (%s|%s|%d): ...).

Risks:

Detailed logs might expose sensitive information (e.g., file paths, commands) if accessible to unauthorized users.

**4. Access to System-Level Functions:**

Observed:

Functions like mmap, ioctl, vfork, execvp.

Paths such as /mnt/mtd/Config/network, /etc/securetty.

Risks:

If improperly implemented, these could lead to privilege escalation or system compromise.

**5. Potential Information Disclosure:**

Observed:

Hardcoded paths (/mnt/mtd/Config/network, /proc/net/dev).

Detailed error messages related to networking (e.g., NetWorkGetMACAddress, NetSetHostIPEx).

Risks:

Paths and error logs may help attackers map the system.

**6. Default or Fixed Security Measures:**

Observed:

Fixed MTU: MTU = 1500.

DHCP configuration in /mnt/mtd/Config/ddns-server.

Risks:

These default settings might be exploitable if not updated during deployment.

**7. Cryptographic Functions:**

- The presence of libcrypt.so.0 and encrypt suggests cryptographic operations. Weak or outdated cryptographic methods could pose security risks.

**8. Stripped Binary:**

- The lack of debugging symbols and limited disassembly indicates the binary is stripped, making it harder to analyze but potentially hiding malicious behavior.

**9. Writable and Executable Sections:**

- The .data and .bss sections are writable, and the .text section is executable. This could allow exploitation via techniques like buffer overflows or return-oriented programming (ROP).  
  
**Next Steps**

1. **Dynamic Execution**:
   * Run the binary in a QEMU ARM emulator with proper monitoring tools (e.g., strace, ltrace) to capture system calls and runtime behavior.
2. **Dependency Analysis**:
   * Investigate /lib/ld-uClibc.so.0 and libcrypt.so.0 for potential vulnerabilities.
3. **Memory Analysis**:
   * Use tools like Valgrind or GDB to detect memory misuse or unsafe operations.
4. **Behavioral Analysis**:
   * Observe the binary's behavior in a sandbox to detect any malicious or unexpected activity.

**Conclusion**

This binary appears to be a stripped ARM executable, likely containing cryptographic functionality and prone to unsafe memory operations. Further dynamic and in-depth analysis is required to fully uncover potential vulnerabilities and risks.