**Problem**

A syntax vulnerability was discovered in the kernel's ASN1.1 DER decoder, which could lead to memory corruption or a complete local denial of service through x509 certificate DER files. A local system user could use a specially created key file to trigger BUG\_ON() in the public\_key\_verify\_signature() function (crypto/asymmetric\_keys/public\_key.c), to cause a kernel panic and crash the system.

**asn1\_decoder.c**

if (op <= ASN1\_OP\_\_MATCHES\_TAG) {

unsigned char tmp;

/\* Skip conditional matches if possible \*/

if ((op & ASN1\_OP\_MATCH\_\_COND && flags & FLAG\_MATCHED) ||

dp == datalen) {

flags &= ~FLAG\_LAST\_MATCHED;

pc += asn1\_op\_lengths[op];

goto next\_op;

}

<https://android.googlesource.com/kernel/common/+/refs/heads/android-mainline/crypto/asymmetric_keys/public_key.c>

public\_key.c: <https://android.googlesource.com/kernel/msm/+/refs/tags/android-8.1.0_r0.24/crypto/asymmetric_keys/public_key.c>

BUG\_ON : <https://elixir.bootlin.com/u-boot/latest/source/include/linux/bug.h#L14>

**Fix**

**asn1\_decoder.c**

if (op <= ASN1\_OP\_\_MATCHES\_TAG) {

unsigned char tmp;

/\* Skip conditional matches if possible \*/

if ((op & ASN1\_OP\_MATCH\_\_COND && flags & FLAG\_MATCHED) ||

(**op & ASN1\_OP\_MATCH\_\_SKIP** && dp == datalen)) {

flags &= ~FLAG\_LAST\_MATCHED;

pc += asn1\_op\_lengths[op];

goto next\_op;

}

<https://docs.huihoo.com/doxygen/linux/kernel/3.7/asn1__ber__bytecode_8h_source.html>

asn1\_ber\_bytecode.h File Reference

Text

Description automatically generated