Case 1:

Code: void* _TIFFmalloc(tmsize_t s) {

    return (malloc((size_t) s));

}

Description: The _TIFFmalloc function in tif_unix.c in LibTIFF 4.0.3 does not reject a zero size, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image that is mishandled by the TIFFWriteScanline function in tif_write.c, as demonstrated by tiffdither.

[output]

SVA-ICL (Code_sim=100%, Text_sim=0%)：High　⊘

SVA-ICL (Code_sim=0%, Text_sim=100%)：Medium　⊗

SVA-ICL (Code_sim=70%, Text_sim=30%)：High　⊘

Ground Truth：High

Case 2:

Code: int Read(void* pDestBuffer, int nSize) {

    if (m_nPos + nSize >= m_nLen)　nSize = m_nLen - m_nPos - 1;

    memcpy(pDestBuffer, (m_sFile + m_nPos), nSize);

    m_nPos += nSize;

    return nSize;

}

Description: Onlyoffice Document Server v6.0.0 and below and Core 6.1.0.26 and below were discovered to contain a heap overflow via the component DesktopEditor/fontengine/fontconverter/FontFileBase.h.

[output]

SVA-ICL (Code_sim=100%, Text_sim=0%)：High　⊗

SVA-ICL (Code_sim=0%, Text_sim=100%)：Medium　⊗

SVA-ICL (Code_sim=70%, Text_sim=30%)：Critical　⊘

Ground Truth：Critical