CVE-2017-5522

描述：Stack-based buffer overflow in MapServer before 6.0.6, 6.2.x before 6.2.4, 6.4.x before 6.4.5, and 7.0.x before 7.0.4 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via vectors involving WFS get feature requests.

软件：MapServer

源码：mapogcfilter.c

出现位置： 3005-3022行

关键源码：

pszValue = psFilterNode->psRightNode->pszValue;

nLength = strlen(pszValue);

iTmp =0;

if (nLength > 0 && pszValue[0] != pszWild[0] &&

pszValue[0] != pszSingle[0] &&

pszValue[0] != pszEscape[0]) {

szTmp[iTmp]= '^';

iTmp++;

}

for (i=0; i<nLength; i++) {

if (pszValue[i] != pszWild[0] &&

pszValue[i] != pszSingle[0] &&

pszValue[i] != pszEscape[0]) {

szTmp[iTmp] = pszValue[i];

iTmp++;

szTmp[iTmp] = '\0';

}