CVE-2017-6349

描述：An integer overflow at a u\_read\_undo memory allocation site would occur for vim before patch 8.0.0377, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows. 软件：

源码：VIM 8.0.0377

出现位置： 1977-1996行

关键源码：

if (num\_head < LONG\_MAX / (long)sizeof(u\_header\_T \*))

uhp\_table = (u\_header\_T \*\*)U\_ALLOC\_LINE(

num\_head \* sizeof(u\_header\_T \*));

if (uhp\_table == NULL)

goto error;

}

while ((c = undo\_read\_2c(&bi)) == UF\_HEADER\_MAGIC)

{

if (num\_read\_uhps >= num\_head)

{

corruption\_error("num\_head too small", file\_name);

goto error;

}

uhp = unserialize\_uhp(&bi, file\_name);

if (uhp == NULL)

goto error;

uhp\_table[num\_read\_uhps++] = uhp; //overflow

}