CVE-2017-6350

描述：An integer overflow at an unserialize\_uep memory allocation site would occur for vim before patch 8.0.0378, 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：VIM

源码：src/undo.c

出现位置：1417-1435 行

关键源码：

if (uep->ue\_size > 0)

{

array = (char\_u \*\*)U\_ALLOC\_LINE(sizeof(char\_u \*) \* uep->ue\_size);

if (array == NULL)

{

\*error = TRUE;

return uep;

}

vim\_memset(array, 0, sizeof(char\_u \*) \* uep->ue\_size);

}

else

array = NULL;

uep->ue\_array = array;

for (i = 0; i < uep->ue\_size; ++i)

{

line\_len = undo\_read\_4c(bi);

if (line\_len >= 0)

line = read\_string\_decrypt(bi, line\_len);

else

{

line = NULL;

corruption\_error("line length", file\_name);

}

if (line == NULL)

{

\*error = TRUE;

return uep;

}

array[i] = line;

}

return uep;

}