CVE-2016-4459

描述：Stack-based buffer overflow in native/mod\_manager/node.c in mod\_cluster 1.2.9.

软件：mod\_cluster 1.2.9.

源码：native/mod\_manager/node.c

出现位置： 222-231行

关键源码：

/\*\*

\* find a node record from the shared table using JVMRoute

\* @param pointer to the shared table.

\* @param node address where the node is located in the shared table.

\* @param route JVMRoute to search

\* @return APR\_SUCCESS if all went well

\*/

apr\_status\_t find\_node(mem\_t \*s, nodeinfo\_t \*\*node, const char \*route)

{

nodeinfo\_t ou;

apr\_status\_t rv;

strcpy(ou.mess.JVMRoute, route);

\*node = &ou;

rv = s->storage->ap\_slotmem\_do(s->slotmem, loc\_read\_node, node, 0, s->p);

return rv;

}