Suricata - Bug #3672
coverity: data directory handling issues
04/24/2020 11:41 AM - Jeff Lucovsky

Status: Closed
Priority: Normal
Assignee: Jeff Lucovsky
Category:
Affected Versions: 5.0.3
Verbose:

### Description
** CID 1460664: (INTERNAL_OVERFLOW)
/src/util-conf.c: 77 in ConfigSetDataDirectory()

```c
71     if (strlen(name) == 0)
72         return TM_ECODE_OK;
73
74     size_t size = strlen(name) + 1;
75     char tmp[size];
76     strlcpy(tmp, name, size);
>>> CID 1460664: (INTERNAL_OVERFLOW)
>>> Overflown or truncated value (or a value computed from an overflown or truncated value)
*size - 2UL" used as array index.
77     if (tmp[size - 2] == '/')
78         tmp[size - 2] = '\0';
79
81 }
82
/src/util-conf.c: 78 in ConfigSetDataDirectory()
71     if (strlen(name) == 0)
72         return TM_ECODE_OK;
73
74     size_t size = strlen(name) + 1;
75     char tmp[size];
76     strlcpy(tmp, name, size);
>>> CID 1460664: (INTERNAL_OVERFLOW)
>>> Overflown or truncated value (or a value computed from an overflown or truncated value)
*size - 2UL" used as array index.
77     if (tmp[size - 2] == '/')
78         tmp[size - 2] = '\0';
79
81 }
82
const char *ConfigGetDataDirectory()
```

### Related issues:
- Copied from Bug #3641: coverity: data directory handling issues

**History**

#1 - 04/24/2020 11:41 AM - Jeff Lucovsky
- Copied from Bug #3641: coverity: data directory handling issues added

#2 - 04/24/2020 02:35 PM - Jeff Lucovsky
- Status changed from Assigned to In Review

https://github.com/OISF/suricata/pull/4869

#3 - 04/25/2020 12:18 PM - Jeff Lucovsky
- Status changed from In Review to Closed