

Bug #18020 CLOSED

Double copyin of dld_ioc consumers

Added by [Dan McDonald](#) 3 months ago. Updated 22 minutes ago.

Status:	Closed	Start date:	
Priority:	Normal	Due date:	
Assignee:	Andy Fiddaman	% Done:	100%
Category:	-	Estimated time:	
Difficulty:	Medium	Gerrit CR:	
Tags:		External Bug:	

Description

Security vulnerability initially discovered for DLC_[GS]ETMACPROP by Nick Wilkens prompting Claude.

This may affect other functions trampolined to by dld_iocctl(). aggr seems to have one too, for example.

History

Notes

Property changes

Updated by [Dan McDonald](#) 8 days ago

There is no mitigation of this issue. The attack vector is timing-dependent and a potential attack can be detected with DTrace. This example script detects one mismatch of the race-window-modified header:

```
#!/usr/sbin/dtrace -s

drv_ioc_prop_common:entry
{ self->header = args[0]; }

drv_ioc_prop_common:return { self->header = NULL; }

ddi_copyin:entry
/ self->header != NULL /
{ self->header2 = args[1]; }

ddi_copyin:return
/self->header2 != NULL/
{
    if (*self->header != *(dld_ioc_macprop_t *) (self->header2)) {
        printf("UNDER 18020 ATTACK pid %d, uid %d, zone %d / %s\n",
            pid, uid, curthread->t_procp->p_zone->zone_id,
            stringof(curthread->t_procp->p_zone->zone_name));
        print(*self->header);
        print(*(dld_ioc_macprop_t *) (self->header2));
        exit(1);
    }
    self->header2 = NULL;
}
```

Updated by [Dan McDonald](#) 8 days ago

Tested successfully against supplied exploit program(s). The DTrace script confirms the attack condition prior to this fix, but if it's run after this fix it will almost always immediately trigger due to the copyin() in drv_ioc_prop_common() not copying the header anymore, but only the data that follows it.



Updated by **Dan McDonald** 8 days ago

- **Assignee** changed from *Dan McDonald* to *Andy Fiddaman*



Updated by **Electric Monk** 8 days ago

- **Status** changed from *New* to *Closed*
- **% Done** changed from *0* to *100*

[git commit 6959feb5b430411a4809b06c53dcdb42fb525eac](#)

```
commit 6959feb5b430411a4809b06c53dcdb42fb525eac
```

```
Author: Dan McDonald <danmcd@edgecast.io>
```

```
Date: 2026-07-08T18:56:39.000Z
```

```
18020 Double copyin of dld_ioc consumers
```

```
Reviewed by: Andy Fiddaman <illumos@fiddaman.net>
```

```
Approved by: Robert Mustacchi <rm+illumos@fingolfin.org>
```



Updated by **Dan McDonald** 8 days ago

- **Private** changed from *Yes* to *No*



Updated by **Andy Fiddaman** 22 minutes ago

This issue has been assigned [CVE-2026-15449](#)