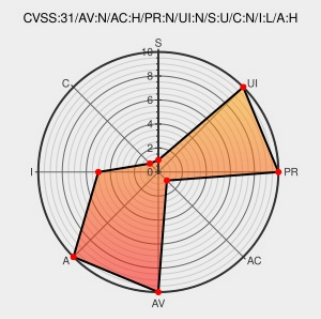
CVE-2020-28713

Published on: 06/08/2021 12:00:00 AM UTC

Last Modified on: 06/21/2021 06:42:00 PM UTC

CVE-2020-28713

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Smart Doorbell from Nightowlsp contain the following vulnerability:

Incorrect access control in push notification service in Night Owl Smart Doorbell FW version 20190505 allows remote users to send push notification events via an exposed PNS server. A remote attacker can passively record push notification events which are sent over an insecure web request. The web service does not authenticate requests, and allows attackers to send an indefinite amount of motion or doorbell events to a user's mobile application by either replaying or deliberately crafting false events.

CVE-2020-28713 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	LOW	HIGH

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
NightOwl Disclosure - GitHub		MISC gist.github.com/ti-oconnor/dbfbaf4d2b271d52fafbd24e1f0024f0

NightOwl Disclosure - GitHub	gist.github.com text/html	MISC gist.github.com/tj-oconnor/dbfbef4d3b27fd53fefbd24e1f002410
Binary Ninja Cloud - Analysis	cloud.binary.ninja text/html	MISC cloud.binary.ninja/embed/26671c64-6859-48fb-b58e-af35dc982b35

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Nightowlsp	Smart Doorbell	-	All	All	All
Operating System	Nightowlsp	Smart Doorbell Firmware	20190505	All	All	All

cpe:2.3:h:nightowlsp:smart_doorbell:-:*:*:*:*:*:*:*:

cpe:2.3:o:nightowlsp:smart_doorbell_firmware:20190505:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-28713 : Incorrect access control in push notification service in Night Owl Smart Doorbell FW version 20190… twitter.com/i/web/status/1…	2021-06-08 19:02:49
/r/netcve	CVE-2020-28713	2021-06-08 19:42:16

← Previous ID Next ID→