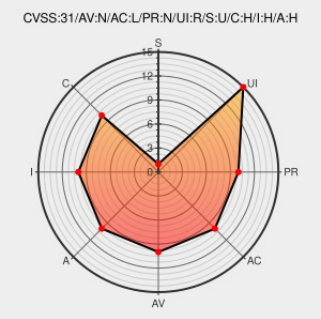
CVE-2020-23592

Published on: Not Yet Published

Last Modified on: 11/23/2022 08:58:00 PM UTC

CVE-2020-23592

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



Certain versions of Op-xt71000n from Optilinknetwork contain the following vulnerability:

A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-191028 allows an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack to Reset ONU to Factory Default through ' /mgm_dev_reset.asp.' Resetting to default leads to Escalation of Privileges by logging-in with default credentials.

CVE-2020-23592 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVE References

Description	Tags	Link
GitHub - huzaifahussain98/CVE-2020-23592: CSRF attack leads to Reset ONU to Factory Default	github.com text/html	MISC github.com/huzaifahussain98/CVE-2020-23592

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

Exploit/POC from Github

CSRF attack leads to Reset ONU to Factory Default

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Optilinknetwork	Op-xt71000n	2.2	All	All	All
Operating System	Optilinknetwork	Op-xt71000n Firmware	3.3.1-191028	All	All	All

cpe:2.3:h:optilinknetwork:op-xt71000n:2.2:*:*:*:*:*:*:*:

cpe:2.3:o:optilinknetwork:op-xt71000n_firmware:3.3.1-191028:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2020-23592 : A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 , Firmware Version: OP_V3.3.1-19102… twitter.com/i/web/status/1…	2022-11-23 02:03:53
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2020-23592 A vulnerability in OPTILINK OP-XT71000N Hardware Version: V2.2 ,… twitter.com/i/web/status/1…	2022-11-23 02:56:02
@JohnJasonFallow	New vulnerability on the NVD: CVE-2020-23592 ift.tt/T7cYWDh	2022-11-23 06:16:54
/r/netcve	CVE-2020-23592	2022-11-23 03:38:47

← Previous ID

Next ID→