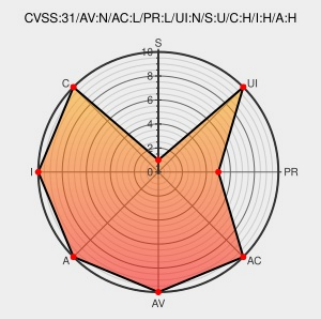
CVE-2020-14076

Published on: 06/15/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:01 PM UTC

CVE-2020-14076

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



Certain versions of Tew-827dru from Trendnet contain the following vulnerability:

TRENDnet TEW-827DRU devices through 2.06B04 contain a stack-based buffer overflow in the ssi binary. The overflow allows an authenticated user to execute arbitrary code by POSTing to apply.cgi via the action st_dev_connect, st_dev_disconnect, or st_dev_rconnect with a sufficiently long wan_type key.

CVE-2020-14076 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	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
IoTFirmware/st_dev_rconnect_overflow.pdf at master · kuc001/IoTFirmware · GitHub	Exploit, Third Party Advisory, github.com	MISC github.com/kuc001/IoTFirmware/blob/master/Trendnet/TEW-827/st_dev_rconnect_overflow.pdf

	text/html	
IoTFirmware/st_dev_disconnect_overflow.pdf at master · kuc001/IoTFirmware · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/kuc001/IoTFirmware/blob/master/Trendnet/TEW-827/st_dev_disconnect_overflow.pdf
IoTFirmware/TRENDnet-st_dev.pdf at master · kuc001/IoTFirmware · GitHub	Third Party Advisory github.com text/html	MISC github.com/kuc001/IoTFirmware/blob/master/Trendnet/TEW-827/TRENDnet-st_dev.pdf
IoTFirmware/st_dev_connect_overflow.pdf at master · kuc001/IoTFirmware · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/kuc001/IoTFirmware/blob/master/Trendnet/TEW-827/st_dev_connect_overflow.pdf

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Trendnet	Tew-827dru	-	All	All	All
Hardware	Trendnet	Tew-827dru	-	All	All	All
Operating System	Trendnet	Tew-827dru Firmware	All	All	All	All

cpe:2.3:h:trendnet:tew-827dru:-:*:*:*:*:*:*:*:

cpe:2.3:h:trendnet:tew-827dru:-:*:*:*:*:*:*:*:

cpe:2.3:o:trendnet:tew-827dru_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→