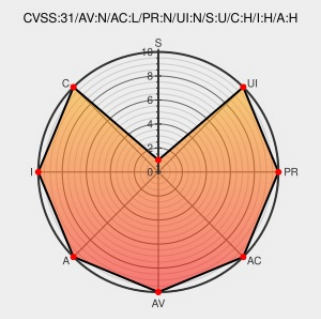
CVE-2020-14080

Published on: 06/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:00 PM UTC

CVE-2020-14080

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 unauthenticated user to execute arbitrary code by POSTing to apply_sec.cgi via the action ping_test with a sufficiently long ping_ipaddr key.

CVE-2020-14080 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
IoTFirmware/ping_test_overflow.pdf at master · kuc001/IoTFirmware · GitHub	Third Party Advisory github.com text/html	MISC github.com/kuc001/IoTFirmware/blob/master/Trendnet/TEW-827/ping_test_overflow.pdf

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

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	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→