CVE-2023-28116

Published on: Not Yet Published

Last Modified on: 03/20/2023 02:46:00 AM UTC

CVE-2023-28116 - advisory for GHSA-m737-4vx6-pfqp

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

Certain versions of Contiki-ng from Contiki-ng contain the following vulnerability:

Contiki-NG is an open-source, cross-platform operating system for internet of things (IoT) devices. In versions 4.8 and prior, an out-of-bounds write can occur in the BLE L2CAP module of the Contiki-NG operating system. The network stack of Contiki-NG uses a global buffer (packetbuf) for processing of packets, with the size of PACKETBUF_SIZE. In particular, when using the BLE L2CAP module with the default configuration, the PACKETBUF_SIZE value becomes larger then the actual size of the packetbuf. When large packets are processed by the L2CAP module, a buffer overflow can therefore occur when copying the packet data to the packetbuf. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. The problem can be worked around by applying the patch manually.

CVE-2023-28116 has been assigned by security-advisories@github.com to track the vulnerability

Affected Vendor/Software: **contiki-ng** - **contiki-ng** version **= <= 4.8**

CVE References

Description	Tags	Link
Prevent buffer overflows due to misconfigured BLE MTU. by nvt · Pull Request #2398 · contiki-ng/contiki-ng · GitHub	github.com text/html	MISC github.com/contiki-ng/contiki-ng/pull/2398
Buffer overflow in L2CAP due to misconfigured MTU · Advisory · contiki-ng/contiki-ng · GitHub	github.com text/html	MISC github.com/contiki-ng/contiki-ng/security/advisories/GHSA-m737-4vx6-pfqp

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Contiki-ng	Contiki-ng	All	All	All	All

cpe:2.3:o:contiki-ng:contiki-ng:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2023-28116 : Contiki-NG is an open-source, cross-platform operating system for internet of things IoT devices… twitter.com/i/web/status/1…	2023-03-17 22:02:50
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2023-28116 Contiki-NG is an open-source, cross-platform operating system for… twitter.com/i/web/status/1…	2023-03-17 22:56:00
/r/netcve	CVE-2023-28116	2023-03-17 22:38:17

← Previous ID

Next ID→