CVE-2020-27213

Published on: Not Yet Published

Last Modified on: 10/10/2023 05:52:00 PM UTC

CVE-2020-27213

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

The following vulnerability was found:

An issue was discovered in Ethernut Nut/OS 5.1. The code that generates Initial Sequence Numbers (ISNs) for TCP connections derives the ISN from an insufficiently random source. As a result, an attacker may be able to determine the ISN of current and future TCP connections and either hijack existing ones or spoof future ones. While the ISN generator seems to adhere to RFC 793 (where a global 32-bit counter is incremented roughly every 4 microseconds), proper ISN generation should aim to follow at least the specifications outlined in RFC 6528.

CVE-2020-27213 has been assigned by cve@mitre.org to track the vulnerability

CVE References

Description	Tags	Link
Ethernut Download	www.ethernut.de text/html	MISC www.ethernut.de/en/download/index.html
En-Nut-Announce Info Page	lists.egnite.de text/html	MISC lists.egnite.de/mailman/listinfo/en-nut-announce
Multiple Embedded TCP/IP Stacks (Update B) | CISA	www.cisa.gov text/html	MISC www.cisa.gov/news-events/ics-advisories/icsa-21-042-01
403 Forbidden	www.forescout.com application/pdf Inactive Link Not Archived	MISC www.forescout.com/resources/numberjack-weak-isn-generation-in-embedded-tcpip-stacks/

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

There are no known software configurations (CPEs) currently associated with this CVE

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→