



CVE-2020-17470

Published on: 12/11/2020 12:00:00 AM UTC

Last Modified on: 10/12/2023 06:31:00 PM UTC

CVE-2020-17470

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Fnet](#) from [Butok](#) contain the following vulnerability:

An issue was discovered in FNET through 4.6.4. The code that initializes the DNS client interface structure does not set sufficiently random transaction IDs (they are always set to 1 in `_fnet_dns_poll` in `fnet_dns.c`). This significantly simplifies DNS cache poisoning attacks.

CVE-2020-17470 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **5.3 - MEDIUM**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
VU#815128 - Embedded TCP/IP stacks have memory corruption vulnerabilities	Third Party Advisory US Government Resource www.kb.cert.org text/html	MISC www.kb.cert.org/vuls/id/815128

No Description Provided

Release Notes

Third Party Advisory

fnet.sourceforge.net

text/html

CONFIRM

fnet.sourceforge.net/manual/fnet_history.html

Multiple Embedded TCP/IP Stacks | CISA

Third Party Advisory

US Government Resource

us-cert.cisa.gov

text/html

MISC

us-cert.cisa.gov/ics/advisories/icsa-20-343-01

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
Application	Butok	Fnet	All	All	All	All
Application	Fnet Project	Fnet	All	All	All	All

cpe:2.3:a:butok:fnet:*.***:*.***:

cpe:2.3:a:fnet_project:fnet:*.***:*.***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →