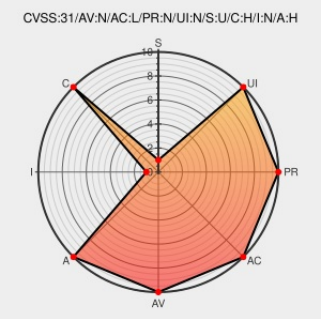
CVE-2020-24383

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

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

CVE-2020-24383

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 for processing resource records in mDNS queries doesn't check for proper '\0' termination of the resource record name string, leading to an out-of-bounds read, and potentially causing information leak or Denial-or-Service.

CVE-2020-24383 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.1 - CRITICAL

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

CVSS2 Score: 6.4 - MEDIUM

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

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

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

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→