



CVE-2018-10238

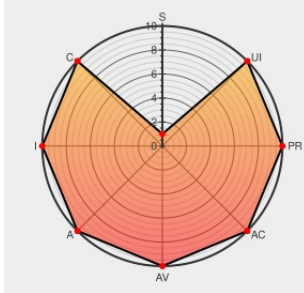
Published on: 04/20/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:21 PM UTC

CVE-2018-10238

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Bacnet Protocol Stack](#) from [Bacnet Protocol Stack Project](#) contain the following vulnerability:

bvlc.c in skarg BACnet Protocol Stack bacserv 0.9.1 and 0.8.5 is affected by a Buffer Overflow because of a lack of packet-size validation. The affected component is bacserv BACnet/IP BVLC forwarded NPDU. The function `bvlc_bdt_forward_npdu()` calls `bvlc_encode_forwarded_npdu()` which copies the content from the

request into a local in the `bvlc_bdt_forward_npdu()` stack frame and clobbers the canary. The attack vector is: A BACnet/IP device with BBMD enabled based on this library connected to IP network. The fixed version is: 0.8.6.

CVE-2018-10238 has been assigned by [M](#) 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
-------------	------	------

SourceForge.net: Log In to SourceForge.net

sourceforge.net
text/html

CONFIRM sourceforge.net/p/bacnet/bugs/55/

BACnet Protocol Stack / SVN-old / Commit [r3168]

Patch
Third Party Advisory
sourceforge.net
text/html

CONFIRM sourceforge.net/p/bacnet/code/3168/

BACnet Protocol Stack / SVN-old / Commit [r3169]

sourceforge.net
text/html

CONFIRM sourceforge.net/p/bacnet/code/3169/

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	Bacnet Protocol Stack Project	Bacnet Protocol Stack	0.8.5	All	All	All
Application	Bacnet Protocol Stack Project	Bacnet Protocol Stack	0.8.5	All	All	All

cpe:2.3:a:bacnet_protocol_stack_project:bacnet_protocol_stack:0.8.5:****:***:

cpe:2.3:a:bacnet_protocol_stack_project:bacnet_protocol_stack:0.8.5:****:***:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→