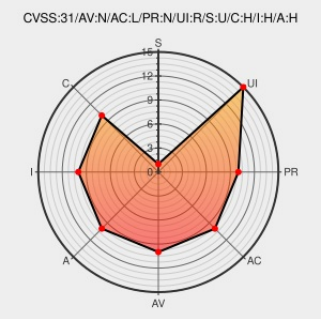
CVE-2019-19720

Published on: 12/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19720

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



Certain versions of Yabasic from Yabasic contain the following vulnerability:

Yabasic 2.86.1 has a heap-based buffer overflow in the yylex() function in flex.c via a crafted BASIC source file.

CVE-2019-19720 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.8 - MEDIUM

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

CVE References

Description	Tags	Link
Heap-based buffer overflow in the yylex() function · Issue #36 · marclhm/yabasic · GitHub	Exploit, Third Party Advisory, github.com, text/html	MISC github.com/marclhm/yabasic/issues/36

Yabasic, Yet another Basic for Unix and Windows

Release Notes
Vendor Advisory
www.yabasic.de
text/html

MISC
www.yabasic.de/whatsnew.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yabasic	Yabasic	2.86.1	All	All	All
Application	Yabasic	Yabasic	2.86.1	All	All	All

cpe:2.3:a:yabasic:yabasic:2.86.1:*:*:*:*:*:*:*:

cpe:2.3:a:yabasic:yabasic:2.86.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→