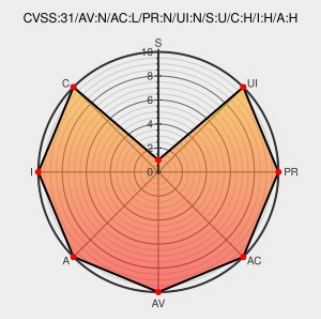
CVE-2020-29311

Published on: 12/10/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-29311

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



Certain versions of Ubilling from Ubilling contain the following vulnerability:

Ubilling v1.0.9 allows Remote Command Execution as Root user by executing a malicious command that is injected inside the config file and being triggered by another part of the software.

CVE-2020-29311 has been assigned by 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: 10 - HIGH

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

CVE References

Description	Tags	Link
u-exploit.png - Google Drive	Exploit Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/file/d/1smOjvenPB-nE0PyIxnfujCT4KcxxkeWV/view?usp=sharing

ubilling-rce.py · GitHub	Exploit Third Party Advisory gist.github.com text/html	MISC gist.github.com/mhaskar/bfa9c2c799fca6697bcc6a213d08cb3e
Ubilling.mp4 - Google Drive	Exploit Issue Tracking Third Party Advisory web.archive.org text/html Inactive Link Not Archived	MISC drive.google.com/file/d/1iLMFSbY8x1CXIf0uFntovY6yZ7N24dQA/view?usp=sharing

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ubilling	Ubilling	1.0.9	All	All	All
Application	Ubilling	Ubilling	1.0.9	All	All	All

cpe:2.3:a:ubilling:ubilling:1.0.9:*:*:*:*:*:*:*:

cpe:2.3:a:ubilling:ubilling:1.0.9:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→