



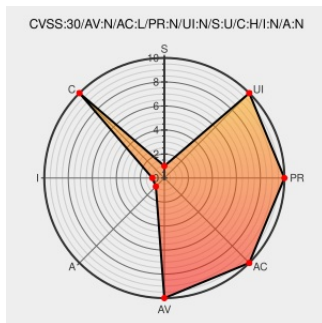
Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-20061

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

Certain versions of [Erpnext](#) from [Frappe](#) contain the following vulnerability:

A SQL injection issue was discovered in ERPNext 10.x and 11.x through 11.0.3-beta.29. This attack is only available to a logged-in user; however, many ERPNext sites allow account creation via the web. No special privileges are needed to conduct the attack. By calling a JavaScript function that calls a server-side Python function with arguments, a SQL attack can be carried out which allows SQL queries to be executed to retrieve any columns from any tables in the database. This is related to CVE-2020-17390. The attack can be performed using the following URLs: `frappe.get_list`, and `frappe.call`.

CVE-2018-20061 has been assigned by [M cve@mitre.org](mailto:cve@mitre.org) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
-------------	------	------

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	Frappe	Erpnext	All	All	All	All
Application	Frappe	Erpnext	11.0.3	beta10	All	All
Application	Frappe	Erpnext	11.0.3	beta11	All	All
Application	Frappe	Erpnext	11.0.3	beta12	All	All
Application	Frappe	Erpnext	11.0.3	beta13	All	All
Application	Frappe	Erpnext	11.0.3	beta14	All	All
Application	Frappe	Erpnext	11.0.3	beta15	All	All
Application	Frappe	Erpnext	11.0.3	beta16	All	All
Application	Frappe	Erpnext	11.0.3	beta17	All	All
Application	Frappe	Erpnext	11.0.3	beta18	All	All
Application	Frappe	Erpnext	11.0.3	beta19	All	All
Application	Frappe	Erpnext	11.0.3	beta2	All	All
Application	Frappe	Erpnext	11.0.3	beta20	All	All
Application	Frappe	Erpnext	11.0.3	beta21	All	All
Application	Frappe	Erpnext	11.0.3	beta22	All	All
Application	Frappe	Erpnext	11.0.3	beta23	All	All
Application	Frappe	Erpnext	11.0.3	beta24	All	All
Application	Frappe	Erpnext	11.0.3	beta25	All	All
Application	Frappe	Erpnext	11.0.3	beta26	All	All
Application	Frappe	Erpnext	11.0.3	beta27	All	All
Application	Frappe	Erpnext	11.0.3	beta28	All	All
Application	Frappe	Erpnext	11.0.3	beta29	All	All
Application	Frappe	Erpnext	11.0.3	beta3	All	All
Application	Frappe	Erpnext	11.0.3	beta4	All	All
Application	Frappe	Erpnext	11.0.3	beta5	All	All


```
cpe:2.3:a:frappe:erpnext:11.0.3:beta10:::*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta11:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta12:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta13:::*:*:*:*:*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta14:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta15:::*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta16:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta17:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta18:*:*:*:*:*:
```

cpe:2.3:a:frappe:erpnext:11.0.3:beta19:*.:*:*:*:*:

cpe:2.3:a:frappe:erpnext:11.0.3:beta2:*:*:*:*:*:

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta20:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta21:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta22:::*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta23:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta24:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta25:::.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta26:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta27:::*:*:*:*:*
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta28:*:*:*:*:*:
```

cpe:2.3:a:frappe:erpnext:11.0.3:beta29:*:*:*:*:*:

cpe:2.3:a:frappe:erpnext:11.0.3:beta3:*:*:*:*:*:

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta4:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta5:*:*:*:*:*:
```

cpe:2.3:a:frappe:erpnext:11.0.3:beta6:*:*:*:*:*:

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta7:*:*:*:*:*:
```

```
cpe:2.3:a:frappe:erpnext:11.0.3:beta8:*:*:*:*:*:
```

cpe:2.3:a:frappe:erpnext:11.0.3:beta9:*:*:*:*:*:

```
cne:2.3:a:franne:ernnext:*.*.*.*.*.*.*.*.*.
```

cpe:2.3:a:frappe:erpnext:11.0.3:beta10:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta11:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta12:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta13:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta14:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta15:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta16:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta17:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta18:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta19:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta2:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta20:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta21:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta22:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta23:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta24:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta25:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta26:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta27:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta28:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta29:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta3:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta4:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta5:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta6:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta7:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta8:*****:
cpe:2.3:a:frappe:erpnext:11.0.3:beta9:*****:

cpe:2.3:a:frappe:erpnext:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)