Risks

# Risks when using community nodes#

Using community nodes means you are installing unverified code from a public source into your n8n instance. This has some risks.

Risks include:

• System security: community nodes have full access to the machine that n8n runs on, and can do anything, including malicious actions.

• Data security: any community node that you use has access to data in your workflows.

• Breaking changes: node developers may introduce breaking changes in new versions of their nodes. A breaking change is an update that breaks previous functionality. Depending on the node versioning approach that a node developer chooses, upgrading to a version with a breaking change could cause all workflows using the node to break. Be careful when upgrading your nodes.

## Report bad community nodes#

You can report bad community nodes to security@n8n.io

## Disable community nodes#

You can disable community nodes by setting N8N\_COMMUNITY\_PACKAGES\_ENABLED to false.

N8N\_COMMUNITY\_PACKAGES\_ENABLED

false