



Critical Gogs RCE Flaw Allows Code Execution by Users

Description

A serious security problem has been found in Gogs, a popular open-source tool for managing code. This problem lets a user run harmful code on the server under certain conditions.

Rapid7, a security company, says this flaw has a score of 9.4. It does not have a special identifier called CVE. The issue happens when a user creates a request with a dangerous name. This can cause the server to run a command that it should not.

Any registered user can create a repo, which is a place to store code. If they turn on a setting called rebase, they can use this flaw quickly and easily. In some cases, a user with access to a repository can also use this problem to run harmful code.

As of now, there is no fix for this issue. It has been reported to the Gogs team. If someone uses this flaw successfully, they can access all repositories and private information.

Rapid7 advises users to stop new registrations and restrict repository creation to fix this issue until a patch is available.

Vocabulary List:

1. **security** //sɪ'kjʊrɪti// (noun): protection from harm or bad actions
2. **flaw** //flɔ// (noun): a mistake or weakness in something
3. **repository** //rɪ'pɒzətɔri// (noun): a place where code or files are stored
4. **restrict** //rɪ'strɪkt// (verb): to limit what people can do or use
5. **patch** //pætʃ// (noun): a small update to fix software problems
6. **access** //æks'sɛs// (verb): to reach or get information or a place

Comprehension Questions

Multiple Choice

1. What is the score given to the security flaw in Gogs by Rapid7?

Option: 7.2



- Option: 8.0
- Option: 9.4
- Option: 10.0

2. What does CVE stand for?

- Option: Common Vulnerability Exposure
- Option: Common Violent Event
- Option: Critical Vulnerability Edge
- Option: Complicated Virus Element

3. What can a user do to potentially exploit the security flaw in Gogs?

- Option: Create a repo
- Option: Change their password
- Option: Turn off rebase
- Option: Use a safe name

4. Which company reported the security issue in Gogs?

- Option: Microsoft
- Option: Google
- Option: Rapid7
- Option: IBM

5. What do users need to stop according to Rapid7's advice?

- Option: Using the tool
- Option: New registrations
- Option: Creating repositories
- Option: Sharing codes

6. Is there a known fix for the security flaw in Gogs at the moment?

- Option: Yes
- Option: No
- Option: In progress
- Option: Not needed

True-False

7. The security flaw in Gogs lets a user run harmful code on the server under certain conditions.



8. Registered users cannot create a repo in Gogs.
9. A user can exploit the flaw without turning on a setting called rebase.
10. Access to all repositories and private information is available if the flaw is successfully used.
11. Gogs has no reported security issues.
12. The Gogs team has been informed about the security problem.

Gap-Fill

13. The security flaw has a score of _____ according to Rapid7.
14. Any registered user can create a _____ in Gogs.
15. Users are advised to restrict _____ creation until a patch is available.
16. As of now, there is no _____ for the security issue in Gogs.
17. A user can exploit the flaw by creating a request with a _____ name.
18. Rapid7 suggests stopping new _____ to mitigate the security issue.

Answer

Multiple Choice: 1. 9.4 2. Common Vulnerability Exposure 3. Create a repo 4. Rapid7 5. New registrations 6. No

True-False: 7. True 8. False 9. False 10. True 11. False 12. True

Gap-Fill: 13. 9.4 14. repo 15. repository 16. fix 17. dangerous 18. registrations

CATEGORY

1. Sci/Tech - LEVEL1

POST TAG

1. critical
2. ESL learning
3. esl news
4. execute
5. gogs



6. Level 1
7. vulnerability

Tags

1. critical
2. ESL learning
3. esl news
4. execute
5. gogs
6. Level 1
7. vulnerability

Date Created

2026/05/29

Author

aimeeyoung99

ESL-NEWS.COM