مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

Actively Exploited Zero-Day Remote Code Execution Vulnerability in Gogs

Tracking #:432318235

Date:13-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed an actively exploited zero-day vulnerability has been identified in Gogs, a widely used self-hosted Git service.

TECHNICAL DETAILS:

An actively exploited zero-day vulnerability has been identified in Gogs, a widely used self-hosted Git service. The vulnerability, tracked as CVE-2025-8110, enables authenticated users to achieve remote code execution (RCE) by abusing symbolic links to bypass a previously deployed security fix. This issue is being exploited in the wild at scale, with more than 700 publicly exposed instances already compromised.

Vulnerability Details

- **CVE-2025-8110**
- **CVSS-BT 8.7 HIGH**
- CVE-2025-8110 is a symbolic-link bypass of an earlier remote code execution vulnerability, CVE-2024-55947, which affected the Gogs PutContents API. The original flaw allowed attackers to abuse path traversal to write files outside the intended Git repository directory. Although the maintainers added input validation to address the path traversal issue, the fix failed to account for the presence of symbolic links within repositories.

Exploitation in the Wild

- Exploitation first observed **July 10, 2025**.
- Confirmed characteristics across compromised servers:
  - Random **8-character repository and owner names**
  - Repositories created shortly before malware execution
  - Evidence of automated, large-scale exploitation
- Scale of exposure:
  - ~1,400 publicly exposed Gogs instances identified
  - **700+ confirmed compromised**

RECOMMENDATIONS:

- All organizations running affected versions of Gogs should apply the available patch immediately to mitigate the risk of active exploitation.
- Gogs instances that were previously exposed to the internet, particularly those with open registration enabled, should be treated as potentially compromised and subjected to a full security and forensic review.
- Administrators should audit all repositories for the presence of suspicious or unexpected symbolic links, especially those referencing paths outside the repository directory.
- The .git/config file and other sensitive configuration files should be reviewed for unauthorized modifications, including injected sshCommand entries.
- Credentials associated with the Gogs service, including SSH keys, access tokens, and service accounts, should be rotated following patch deployment.
- Until patching is completed, repository creation privileges should be restricted to trusted users only.

- Network exposure should be reduced by placing Gogs behind a VPN, reverse proxy, or IP allow-list where possible.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-8110
- https://github.com/gogs/gogs/pull/8078