Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

The Gogs Blind Spot: A Zero-Day Fueled Mass Compromise

Date of Publication	Last Update Date	Admiralty Code	TA Number
December 12, 2025	February 4, 2026	A1	TA2025377

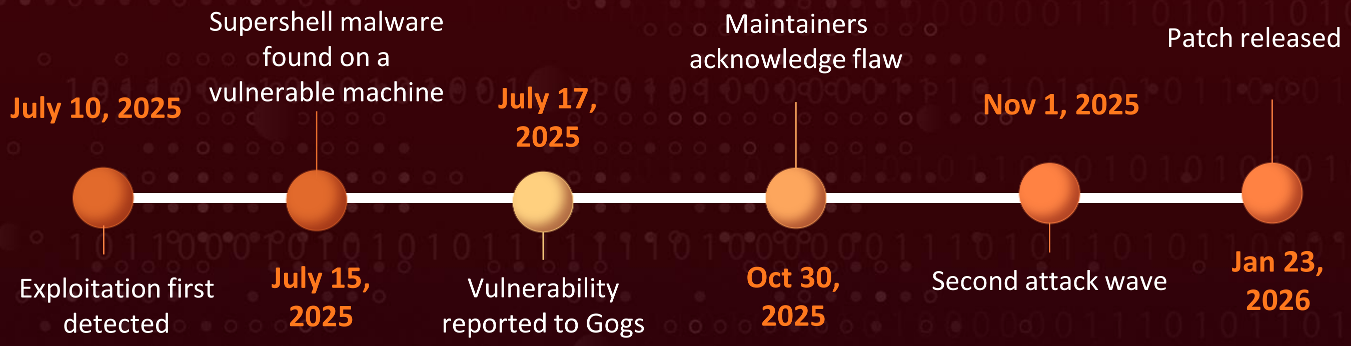
Summary

Discovered On: July 10, 2025
Affected Products: Gogs
Malware: Supershell
Impact: A newly identified zero-day vulnerability (CVE-2025-8110) in Gogs, the widely used self-hosted Git platform, allows authenticated users to achieve remote code execution through improper symbolic-link handling in the PutContents API, effectively sidestepping the previous fix for CVE-2024-55947. Following its disclosure, investigators confirmed active malware deployments and found that more than 700 of roughly 1,400 exposed Gogs instances had already been compromised. Exploitation has been underway since at least July 10, 2025, with attackers leveraging the Supershell open-source C2 framework.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-8110	Gogs Path Traversal Vulnerability	Gogs	✓	✓	✓
CVE-2024-55947	Gogs Path Traversal Vulnerability	Gogs	✗	✗	✓

Exploitation Timeline



July 10, 2025
Exploitation first detected

July 15, 2025
Supershell malware found on a vulnerable machine

July 17, 2025
Vulnerability reported to Gogs

Oct 30, 2025
Maintainers acknowledge flaw

Nov 1, 2025
Second attack wave

Jan 23, 2026
Patch released

Vulnerability Details

#1

A newly discovered zero-day flaw in Gogs surfaced on July 10, when investigators identified active malware infections across multiple public-facing instances. What initially appeared to be an isolated compromise quickly revealed itself as an ongoing exploitation campaign targeting an unknown vulnerability. The issue was immediately disclosed to Gogs maintainers, who began working on a fix, but the exploitation remains active, leaving hundreds of deployments exposed to a serious threat.

#2

Gogs, a lightweight Git service written in Go, is widely used as a streamlined alternative to GitLab or GitHub Enterprise. Its simplicity and portability have made it popular across both on-premise and cloud environments, supporting development teams in remote and distributed setups. That same popularity, however, has expanded its attack surface: more than 1,400 Gogs servers are publicly reachable, and many still allow “Open Registration” by default. This combination of misconfiguration and broad exposure created ideal conditions for threat actors to weaponize the newly uncovered flaw.

#3

The vulnerability, now tracked as CVE-2025-8110, functions as a bypass for a previously addressed remote code execution issue, CVE-2024-55947. Although maintainers attempted to patch the earlier path traversal flaw by validating user-supplied input, they did not account for symbolic links within Git repositories. Because Gogs allows symlinks that point outside the repository, attackers can abuse the PutContents API to overwrite arbitrary files beyond the intended directory. By modifying sensitive files such as .git/config, specifically the sshCommand field, an attacker can execute arbitrary commands on the host. This oversight reflects a recurring architectural weakness in Gogs’ handling of symlinks, like issues observed in CVE-2024-56731 and CVE-2024-54148.

#4

The initial breach involved a compromised cloud workload running Gogs v0.13.2, a version previously believed to be protected against earlier RCE vulnerabilities. The server contained suspicious repositories created days before the malware infection, each named using random eight-character strings, clear evidence of automated exploitation. The malware deployed across these hosts was Go-based, UPX-packed, and heavily obfuscated with Garble. Once deobfuscated using Mandiant’s ungarbler, it was identified as part of the Supershell framework, a tool used to establish reverse SSH shells for remote command execution. The campaign ultimately traced back to a single Command-and-Control server, strongly suggesting a coordinated and large-scale attack carried out by one actor or a closely aligned group.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-8110	Gogs (Prior to 0.13.4, all versions through 0.13.3)	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	CWE-22
CVE-2024-55947	Gogs Versions Prior to 0.13.1	cpe:2.3:a:gogs:gogs:*:*:*:*:*:*:*:*	CWE-22

Recommendations

Patch Gogs: Apply the official update immediately. A fix has been issued in version v0.13.4; update to the latest version as soon as possible.

Disable "Open Registration" On All Gogs Instances: Prevent attackers from creating unauthorized accounts by turning off public sign-ups, especially on internet-facing servers.

Audit All Repositories For Suspicious Symlinks: Look for symbolic links pointing outside the repo directory. Remove anything unexpected and monitor for new creations.

Check For Signs Of Compromise: Review recent repository names, unexpected new users, modified .git/config files, or eight-character random repo names; these were common indicators in this campaign.

Enable Logging and Central Monitoring: Turn on detailed Gogs logs and forward them to your SIEM. Early visibility helps detect exploitation attempts quickly.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0011 Command and Control	T1190 Exploit Public-Facing Application	T1059 Command and Scripting Interpreter
T1505 Server Software Component	T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1071 Application Layer Protocol
T1588 Obtain Capabilities	T1588.006 Vulnerabilities		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	d8fcd57a71f9f6e55b063939dc7c1523660b7383, efda81e1100ea977321d0f2eeb0dfa7a6b132abd
IPv4	119[.]45[.]176[.]196, 106[.]53[.]108[.]81, 119[.]91[.]42[.]53

Patch Link

https://github.com/gogs/gogs/releases

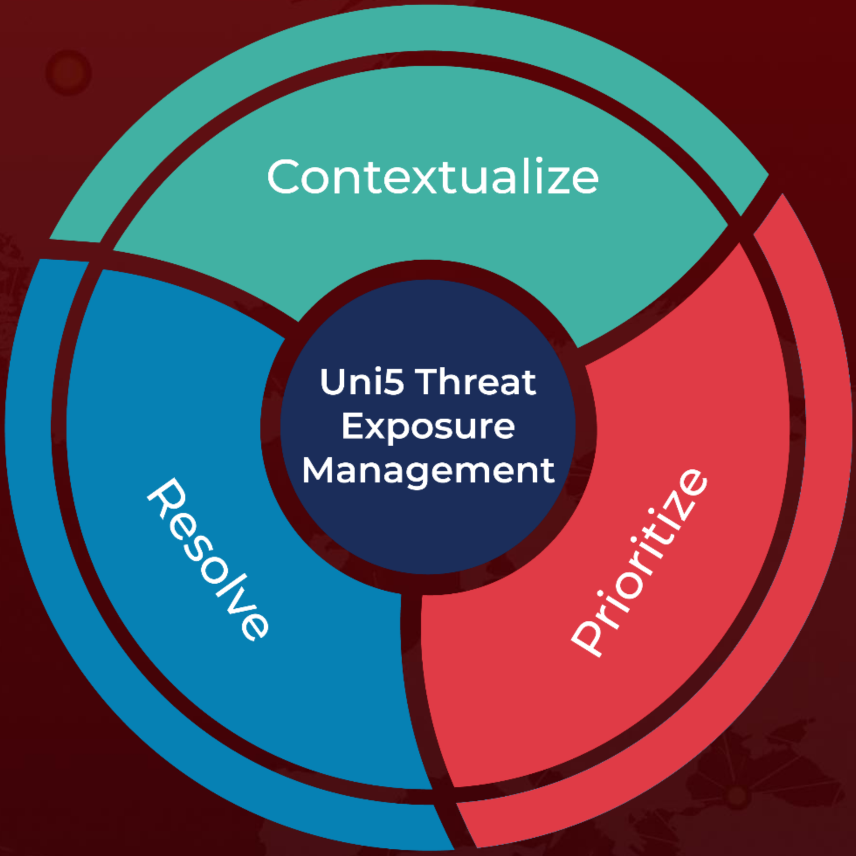
References

https://www.wiz.io/blog/wiz-research-gogs-cve-2025-8110-rce-exploit

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

December 12, 2025 • 8:30 AM

More at www.hivepro.com