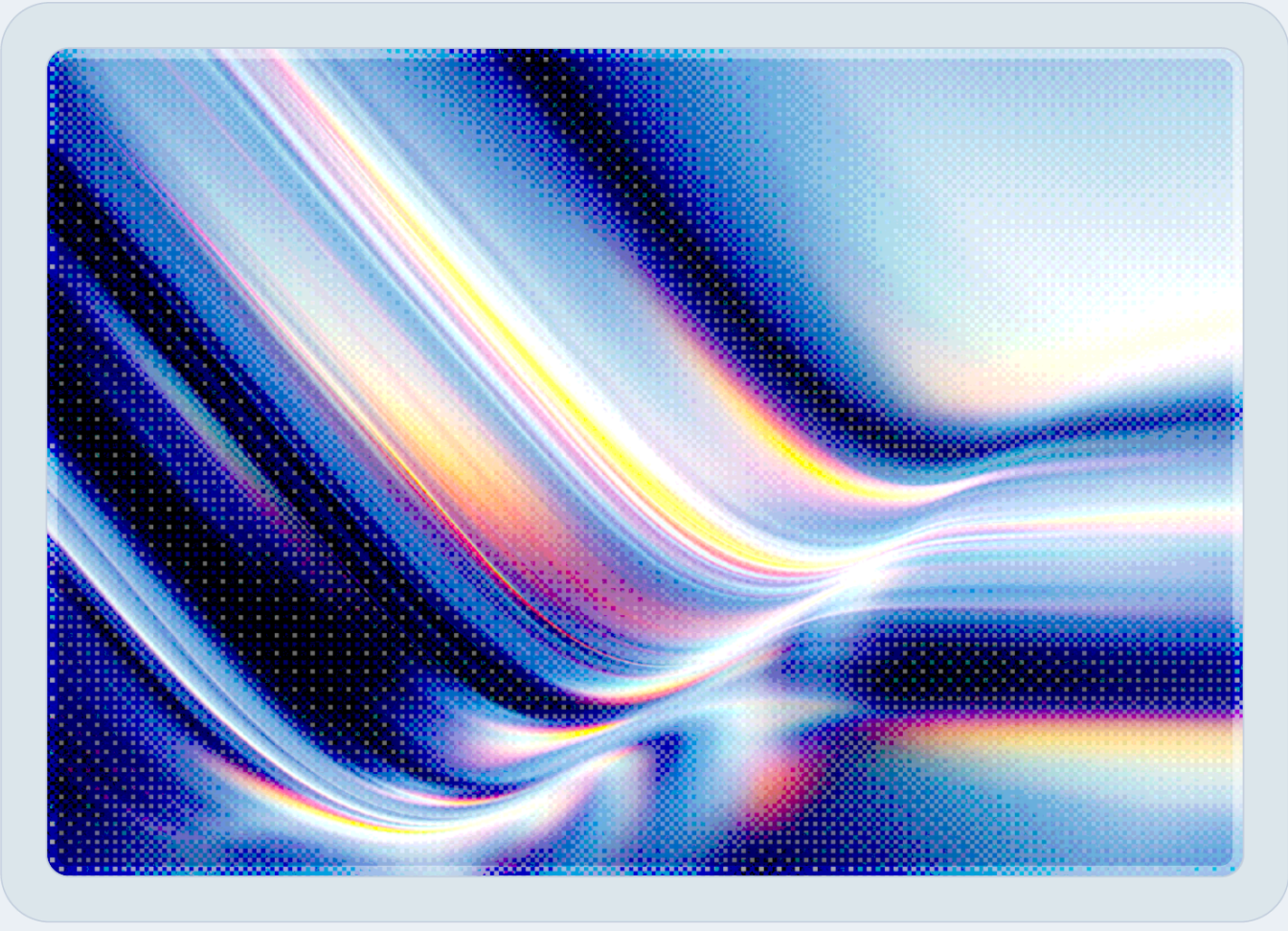
CSAI Foundation | Cloud Security Alliance

Red Heron Weaponizes Gitea RCE, Compromises 13 Organizations

China-Linked Actor Turns an N-Day Flaw Into a Global Espionage Tool

2026-09-16

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

A suspected China-linked threat actor tracked by Acronis's Threat Research Unit as Red Heron converted a public proof-of-concept for CVE-2026-60004, a critical remote code execution flaw in the Gitea source-code hosting platform, into a working exploitation framework within two days of the vulnerability's disclosure, and used it to scan more than 1,300 internet-facing Gitea instances across seven countries [1][2]. That reconnaissance produced confirmed compromises spanning defense, elections, energy, aerospace, telecommunications, government, public safety, and research sectors. The two lead sources on this campaign report somewhat different totals: The Hacker News puts the confirmed count at thirteen organizations across six countries, while Acronis TRU's own technical report counts eleven confirmed compromises across five countries and treats an additional Qatar-based incident as an unconfirmed exfiltration attempt rather than a confirmed compromise [1][2]. Background, Table 1 breaks down both counts by country. The speed of weaponization, roughly 48 hours from public disclosure to an automated attack tool, illustrates how quickly this particular n-day vulnerability converted into operational access for a capable adversary, leaving defenders a shrinking window to patch before exploitation began in earnest.

Beyond initial access, Red Heron deployed a previously undocumented toolset: a C++ Linux implant called JITTERLY that supports more than thirty post-exploitation commands, paired with an LD_PRELOAD-based rootkit called SIXZUT that hides files, processes, and network connections from standard administrative tools [1][2]. Victims documented so far include a Taiwanese industrial automation firm from which hundreds of SCADA and HMI-related repositories were exfiltrated, and an energy-sector target where the actor collected configuration secrets, internal tokens, and SSH host keys [1]. Because Gitea and similar self-hosted code-collaboration platforms sit upstream of build pipelines, credentials, and operational technology configuration data, organizations running exposed instances should treat this campaign as a concrete demonstration that source-code repositories can be a front-line espionage target, not merely a productivity tool, and should act on the credential-rotation and forensic guidance below regardless of whether Red Heron specifically has been observed in their environment.

Background

Gitea is a commonly used, self-hosted alternative to GitHub and GitLab, used by enterprises, government agencies, and open-source projects that prefer to keep source-code hosting inside their own infrastructure rather than relying on a third-party cloud service. That self-hosting model is also what makes Gitea instances attractive targets: unlike centrally managed SaaS platforms, self-hosted Gitea deployments depend entirely on individual organizations to track disclosures and apply patches promptly, and many instances are exposed directly to the internet to support distributed development teams or open registration for external contributors.

CVE-2026-60004 is a critical (CVSS 9.8) remote code execution vulnerability affecting Gitea versions 1.17 through 1.27.0, rooted in how the platform's diffpatch API processes repository patches [3][4]. An attacker with ordinary write access to a repository, which on many instances requires nothing more than registering a free account, can submit a crafted patch twice in succession: the first submission places a malicious payload into Git's index, and the second triggers an "add/add" collision that forces Git's three-way merge logic to write that payload into the repository's hook directory. Because the temporary clone Gitea uses during this process is a bare repository, its root doubles as the active Git directory, so a file written to the hook path executes automatically the next time Git performs an index-related action, running with the privileges of the Gitea service account [3][4]. Gitea's maintainers disclosed the flaw and released the fix, version 1.27.1, on July 27, 2026, and CSA published an earlier research note documenting the vulnerability's mechanics and initial cryptomining-driven exploitation shortly after CISA added it to the Known Exploited Vulnerabilities catalog on August 25, 2026, with a federal remediation deadline of August 28 [5][8]. That first wave of exploitation was largely opportunistic. The campaign described here represents a materially different threat: a capable, apparently state-aligned actor using the same vulnerability for targeted intelligence collection rather than commodity cryptomining.

Acronis TRU's tracking shows Red Heron cloning the public proof-of-concept exploit on July 28, 2026, one day after Gitea's disclosure and patch release, and iterating on it directly before completing a scan of 1,386 Gitea instances across seven countries by July 30, 2026, and compiling a separate target list of 477 Taiwan-based systems the following day [1][2]. Batch exploitation against selected targets followed in early August, with affected sectors including defense and military-linked organizations, election infrastructure, energy providers, aerospace, telecommunications, government agencies, public safety entities, and research institutions [1].

The two primary sources for this campaign disagree on the exact confirmed-compromise total. The Hacker News reports thirteen organizations across six countries, including one Qatar-based victim. Acronis TRU, the primary technical source used throughout the rest of this note, counts eleven confirmed compromises across five countries and characterizes the Qatar incident as an unconfirmed

exfiltration attempt observed during automated batch reconnaissance rather than a confirmed compromise. Table 1 presents both counts by country. Neither figure is disqualifying, but readers relying on this note for incident-response prioritization should treat the eleven confirmed, independently detailed compromises as the more conservative baseline, with the additional two as plausible but unconfirmed.

Table 1. Confirmed Red Heron Compromises by Country, Per Source

Country	The Hacker News [1]	Acronis TRU [2]
Canada	2	2
United States	4	2
Taiwan	4	3
Argentina	1	1
Qatar	1	0 (unconfirmed exfiltration attempt)
Sri Lanka	1	1
Total	**13**	**11**

Security Analysis

Attribution of Red Heron rests on operational artifacts rather than infrastructure overlap with previously tracked groups. Acronis researchers assess with moderate confidence that the actor operates within a China-linked context, citing the use of Simplified Chinese-language labels in the actor's own targeting datasets, categories such as "defense/military-linked" and "election/voting systems" applied to victim organizations, and a convention of classifying Taiwan as part of China (labeled "CN") rather than as a distinct country in those same datasets [1][2]. In CSA's own analytical reading, the targeting pattern, concentrated on defense, energy, and election-adjacent organizations across multiple continents, is consistent with the kind of strategic collection priorities historically associated with Chinese state-linked intrusion sets; that comparison is CSA's observation rather than a claim made in Acronis's report. Acronis itself found no direct technical links to any previously named advanced persistent threat group, and the attribution should be read as an informed assessment rather than a confirmed identification.

The post-exploitation toolset Red Heron deployed is more novel than the initial access vector. JITTERLY, the primary implant, is written in C++ for Linux and supports more than thirty commands covering shell execution, file transfer in throttled chunks, interactive pseudo-terminal sessions, and SOCKS-based network tunneling that allows the operator to pivot deeper into a victim's internal network from a single compromised Gitea host [1][2]. Command-and-control traffic is encrypted with AES-128-GCM over raw TCP [1][2], a transport choice that avoids the more easily fingerprinted patterns of HTTP-based beacons many network detection tools are tuned to catch. Paired with JITTERLY is SIXZUT, an LD_PRELOAD rootkit that Acronis describes as previously undocumented, which conceals the implant's files, processes, and network connections by patching roughly fifteen Linux library functions that administrative and monitoring tools rely on to enumerate system state [1][2]. Because SIXZUT installs itself via /etc/ld.so.preload and actively relaunches the implant if it is killed while the rootkit binary remains on disk, Acronis's guidance to defenders is unusually blunt: attempting to clean a compromised host in place is unreliable, and organizations that find SIXZUT artifacts should plan to rebuild the affected system rather than remediate it [1][2].

The escalation from initial repository access to this level of persistence is illustrated by the Taiwanese industrial automation victim, where The Hacker News reports the actor exfiltrated hundreds of repositories related to SCADA and HMI systems before achieving root-level administrative access across a three-node Proxmox virtualization cluster; this level of detail was not independently corroborated in Acronis's own published account [1]. At an energy-sector victim, the actor's collection focused on configuration secrets, internal authentication tokens, and SSH host keys rather than source code alone, indicating an interest in infrastructure mapping and future access rather than a one-time data theft; as with the Taiwanese case, this specific detail is drawn from The Hacker News's reporting rather than independently corroborated elsewhere [1]. Notably, the same staging server Red Heron used for Gitea exploitation had previously been used to target eighteen Joomla-based websites across ten countries, suggesting the actor runs a broader, opportunistic scanning operation in parallel with more deliberately targeted campaigns against specific sectors [1][2]. That dual pattern, indiscriminate scanning layered with structured target selection against strategically relevant organizations, is, in CSA's own analysis, consistent with how several state-linked actors have operated against other n-day vulnerabilities in internet-facing software over the past several years; this comparison, too, is CSA's observation rather than a claim documented by Acronis. It means organizations should not assume that being caught up in a mass-scanning sweep is a lesser event than being deliberately targeted; either can lead to the same implant and rootkit landing on a production host.

Recommendations

Immediate Actions

Organizations running any Gitea instance still on version 1.27.0 or earlier should treat patching to 1.27.1 or later as an active incident response action rather than a routine update, given that both opportunistic cryptomining actors and Red Heron have had roughly seven weeks to exploit unpatched instances since disclosure [3][4][5]. Any instance that was internet-facing and unpatched at any point since late July 2026 should be treated as potentially compromised until proven otherwise: administrators should check for unauthorized entries in Git hook directories, review account creation logs for registrations around late July and early August, and inspect /etc/ld.so.preload for unauthorized entries such as a library masquerading under a name like "libglthread.so.2," which Acronis observed SIXZUT using for persistence [1][2]. Given SIXZUT's demonstrated ability to hide its own artifacts from standard filesystem and process-enumeration tools, any positive indicator from these checks, or any inability to rule out compromise with confidence, should trigger a full rebuild of the affected host rather than an in-place cleanup.

Short-Term Mitigations

Because the underlying vulnerability required only ordinary repository write access, and many Gitea deployments allow open self-registration by design, organizations should disable open registration on internet-facing instances or restrict it behind an approval workflow, independent of whether they have already patched, to reduce the attack surface for both this vulnerability class and future ones that depend on low-privilege account creation. Any credentials, API tokens, or SSH keys that were accessible to a Gitea instance exposed during the vulnerability window should be rotated as a precaution, since Red Heron's apparent objective, based on the data types the actor is documented to have collected, included harvesting exactly this kind of material for lateral movement rather than source code alone [1]. Security teams should also extend log review beyond the Gitea host itself to any systems that host reused credentials or trust relationships with it, including build servers, container registries, and, for organizations in sectors like the Taiwanese industrial automation victim, any operational technology management interfaces that share administrative credentials with development infrastructure.

Strategic Considerations

This campaign is consistent with the disclosure-to-exploitation compression CSA flagged in its prior analysis of this same vulnerability: the roughly 48-hour gap between Gitea's July 27 patch release and Red Heron's working attack tool left organizations that rely on standard patch-cycle timelines exposed during precisely the window when the most capable actors were moving fastest [5]. Confirming that this compression reflects a broader trend across n-day exploitation generally, rather than a dynamic specific to this vulnerability, would benefit from additional independent data points beyond this single campaign. Development infrastructure such as source-code hosting platforms, CI/CD systems, and artifact registries nonetheless deserves the same asset-inventory rigor and priority patching treatment that organizations typically reserve for internet-facing production systems, since compromise of a code-hosting platform can expose credentials, secrets, and design details for everything built on top of it, including, in this campaign, industrial control system configurations. Organizations in defense, energy, elections, and other sectors that appeared among Red Heron's confirmed victims or scanning targets should also weigh threat-informed defense investments, such as monitoring for the specific detection indicators Acronis has published, more heavily than generic vulnerability-management metrics alone would suggest, given Acronis's assessment, at moderate confidence, that a state-linked actor is deliberately pursuing their sector.

CSA Resource Alignment

This campaign is a direct continuation of the vulnerability CSA analyzed in its earlier research note, Gitea RCE Under Active Exploitation: CVE-2026-60004, published August 26, 2026, which covered the vulnerability's technical mechanics, its addition to CISA's KEV catalog, and the initial wave of opportunistic cryptomining exploitation [5]. That note's guidance to treat Gitea as Tier-1 infrastructure with production-grade patch management applies with even greater force now that a state-linked actor has demonstrated targeted, espionage-oriented use of the same flaw; organizations that deferred remediation on the assumption that opportunistic exploitation posed limited risk should revisit that assessment in light of Red Heron's documented sector-specific targeting.

The speed at which Red Heron weaponized CVE-2026-60004, moving from public disclosure to an automated exploitation framework within roughly 48 hours, mirrors the dynamic documented in CSA's Project Glasswing: AI Discovery Outpaces Open Source Patching Capacity, which examined how the compression of the discovery-to-exploitation timeline is outpacing organizations' ability to patch open-source infrastructure at human speed [6]. Defenders evaluating how quickly they could realistically have

patched an internet-facing Gitea instance between July 27 and July 29, 2026, should use that report's framing to judge whether their current patch-management tooling is built for this compressed timeline or for a slower, pre-automation threat model.

Because confirmed Red Heron victims include a Taiwanese industrial automation company from which SCADA and HMI repositories were stolen, and an energy-sector organization targeted for infrastructure secrets, this incident also falls within the scope of CSA's Zero Trust Guidance for Critical Infrastructure, which addresses how Zero Trust principles apply to operational technology and industrial control system environments [7]. Organizations that maintain shared credentials or trust relationships between development infrastructure and OT/ICS management systems, the exact pattern that allowed source-code compromise to translate into broader infrastructure exposure in this campaign, should treat that guidance's segmentation recommendations as directly applicable to closing the pathway this campaign exploited.

References

[1] The Hacker News. "Red Heron Exploits Gitea RCE to Compromise 13 Organizations Across Six Countries." The Hacker News, September 2026.

[2] Acronis. "Red Heron Exploits Gitea N-Day Flaw in Multinational Campaign, Exposing New Linux Rootkit." Acronis Threat Research Unit, September 2026.

[3] GitLab Advisory Database. "CVE-2026-60004: Gitea Remote Code Execution via diffpatch Git Hook Installation." GitLab, 2026.

[4] The Hacker News. "Critical Gitea RCE Actively Exploited as Reported Attack Drops Miner-Like Payload." The Hacker News, August 2026.

[5] Cloud Security Alliance. "Gitea RCE Under Active Exploitation: CVE-2026-60004." Cloud Security Alliance AI Safety Initiative, August 26, 2026.

[6] Cloud Security Alliance. "Project Glasswing: AI Discovery Outpaces Open Source Patching Capacity." Cloud Security Alliance, 2026.

[7] Cloud Security Alliance. "Zero Trust Guidance for Critical Infrastructure." Cloud Security Alliance, 2025.

[8] SecurityWeek. "CISA Warns of Exploited Gitea Vulnerability." SecurityWeek, August 2026.

