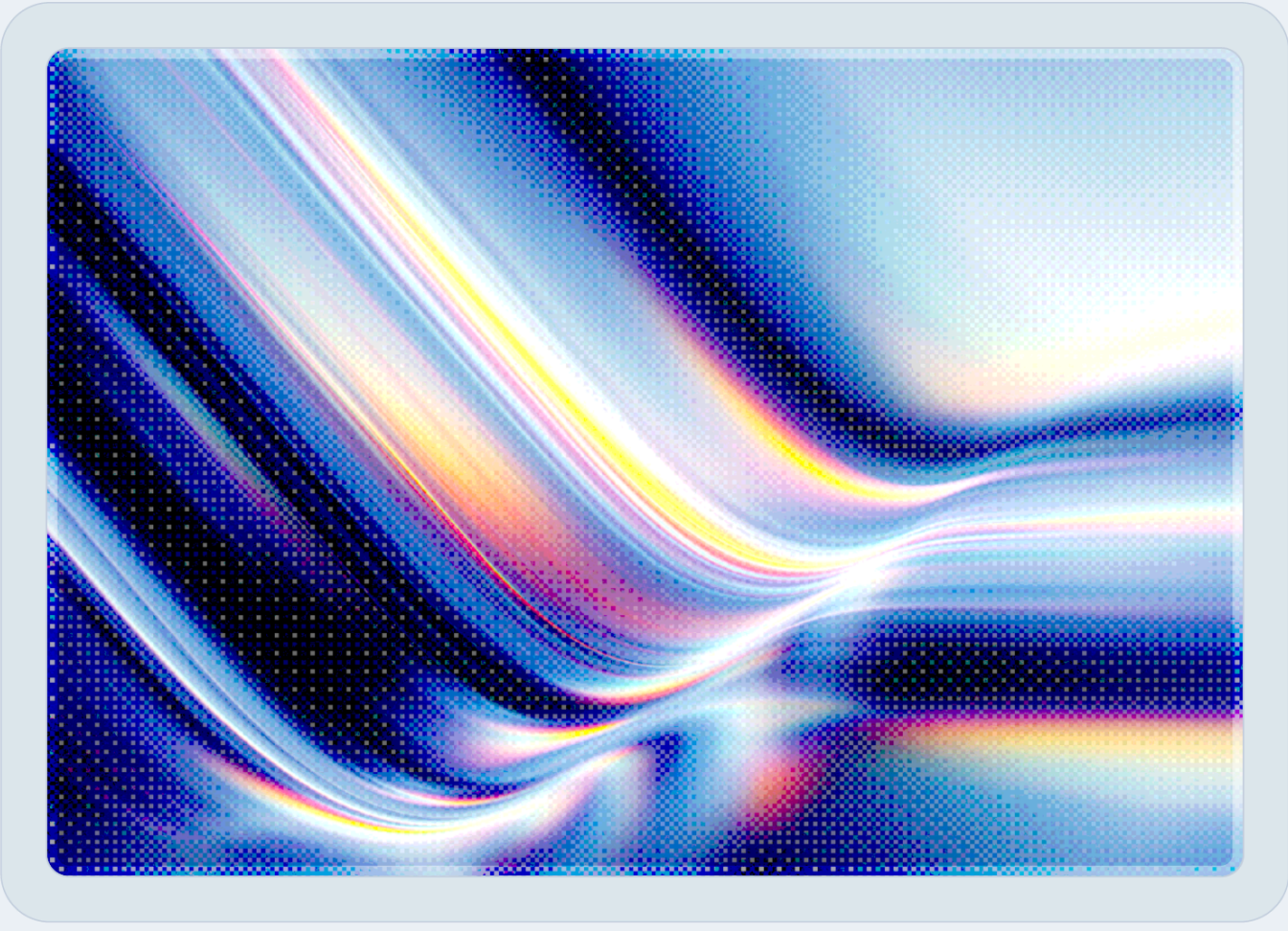
CSAI Foundation | Cloud Security Alliance

GeoServer Under Active Exploitation: KEV-Listed RCE Chains and the WeaveLotus Campaign

Security Implications and Guidance for Operators of Geospatial Data Services

2026-11-29

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

© 2026 Cloud Security Alliance. Some rights reserved.

You may download, store, display, view, print, redistribute, and link to this document in its original, unmodified form, provided that attribution to the Cloud Security Alliance is maintained and all trademark and copyright notices remain intact.

This document may not be modified or altered. You may quote portions of the document as permitted by the Fair Use provisions of the United States Copyright Act, provided that attribution is given to the Cloud Security Alliance.

This document may be shared on professional and social media platforms in its original form with attribution.

This document was generated with AI assistance and has not undergone official CSA review and approval processes.

Key Takeaways

Attackers are exploiting two GeoServer flaws: CVE-2026-120705 (CVSS 8.6), an unauthenticated XML injection in the Web Feature Service (WFS) that allows local file reads and server-side request forgery, and CVE-2026-129243 (CVSS 8.8), an authorization bypass triggered by prefixing a service name. CISA added both to its Known Exploited Vulnerabilities (KEV) catalog on November 27, 2026 [2], and the catalog entries set a November 30, 2026 remediation deadline for federal civilian agencies [16]. Independent researchers have also published working chains that lead from an anonymous request to code execution on the host. Those chains combine the two exploited flaws with a predictable "remember-me" signing key (CVE-2026-129245, CVSS 9.2) and code execution through admin-only JDBC features (CVE-2026-120704 or CVE-2026-129242) [3][5][9][10].

Fixes are available in GeoServer 2.27.7, 2.28.6, and 3.0.2, and CVE-2026-120705 additionally requires the matching GeoTools releases. The fixed releases shipped between October and early November 2026, with Eye Security reporting availability from October 19, yet the advisories were not published until November 23–24 [1][3][9]. Because the file-read primitive exposes both the administrator password digest and the remember-me key, patching alone does not undo credential exposure that has already occurred, and any server exposed while unpatched should be treated as potentially compromised [5].

The threat extends beyond the November disclosures. SOCRadar documented a suspected Vietnam-linked intrusion set, WeaveLotus, that used exposed open-source applications, including GeoServer, JasperReports, osTicket, and Laravel, as initial-access footholds against Southeast Asian government, military, and legislative organizations [11][12]. In that campaign the GeoServer intrusion likely relied on the 2024 flaw CVE-2024-36401 rather than the November 2026 vulnerabilities [11]. GeoServer has been exploited repeatedly since 2024, including CVE-2024-36401 and an August 2026 zero-day [13][14]. Geospatial servers can feed analytics and AI data pipelines and are frequently managed outside central IT, so organizations should treat them as high-value, internet-facing infrastructure rather than as niche GIS tooling.

Background

GeoServer is an open-source Java server that publishes geospatial data using Open Geospatial Consortium (OGC) standards. These include the Web Map Service (WMS), the Web Feature Service (WFS), and the Web Coverage Service. Its users include national mapping agencies, defense and civil government bodies, utilities, environmental and agricultural agencies, logistics operators, and research institutions. In many of these settings GeoServer is installed by a GIS or data-science team rather than by central IT. It is often exposed directly to the internet so that partner organizations and public map viewers can consume its layers. Eye Security reported identifying more than 3,000 internet-accessible GeoServer instances during its research [9]. Because many deployments sit on internal networks or behind partner-facing gateways, that figure likely understates the real installed base.

GeoServer has been a recurring exploitation target. In July 2024, CISA added CVE-2024-36401 to the KEV catalog. That flaw is a critical (CVSS 9.8) remote code execution vulnerability in how GeoServer evaluates OGC property names [13]. In August 2026, watchTowr observed hundreds of exploitation attempts within hours of disclosure of CVE-2026-76904. That flaw is an unauthenticated SQL injection in the PostGIS data store's `jsonArrayContains` function, fixed in 3.0.1, 2.28.5, and 2.27.6 [14]. The vulnerabilities disclosed in November 2026 continue the pattern. Eye Security states that it found its chain with AI assistance [9]. This is consistent with the trend CSA has described, in which AI-assisted research increases the volume of discovered vulnerabilities and shortens exploitation windows [18].

The November cluster's timeline matters because it shows how long the quiet window between fix and disclosure lasted. Eye Security reported its findings to the maintainers on September 29, 2026, and reports that fixed releases were available from October 19 [9]; GitHub release records show the three fixed branches shipping between October 17 and November 2 [15]. Separately, Rapid7 researcher Jonah Burgess (CryptoCat) independently reported a five-step chain on August 2, 2026, roughly eleven weeks before the first fixed releases shipped [1][10]. The GeoServer project published its GitHub security advisories on November 23–24 [3][4][5]. watchTowr reported exploitation against its honeypot network early on November 25 [1], and CISA added the two entry-point CVEs to KEV two days later [2]. The quiet window between fix and disclosure therefore lasted about five weeks. Organizations that applied the October and early-November maintenance releases were protected before the advisories appeared, provided their GeoTools components were updated in step. Organizations that waited for an advisory before patching had roughly a day before exploitation attempts were observed [1].

Security Analysis

The Vulnerabilities

The November advisories cover six CVEs that work as building blocks for each other. No single flaw yields unauthenticated code execution on its own. Taken together, they turn an anonymous WFS request into full control of the GeoServer host. The table below summarizes each flaw as described in the GeoServer project's GitHub security advisories and in the researchers' write-ups.

CVE	Severity	Description	Role in chains
CVE-2026-129244	6.9	WFS stored-query exception discloses the data directory path [7]	Reconnaissance: tells the attacker where target files live
CVE-2026-129243	8.8 (KEV)	Service security rules bypassed using a prefixed service name such as `x/WFS`, letting anonymous users create and delete stored queries [4]	Access: reaches admin-only stored-query operations
CVE-2026-120705	8.6 (KEV)	Unauthenticated WFS GetFeatureById XML injection; XInclude elements allow reading local files and fetching attacker-chosen URLs (SSRF) [3]	Disclosure: reads `users.xml` and `security/config.xml`
CVE-2026-129245	9.2	Remember-me cookie signing key read from `security/config.xml`; the shipped default is the string `geoserver`, which most installations never change [5]	Escalation: forges an administrator session without cracking the password
CVE-2026-120704	7.2	Improper control of code generation in JDBC security configuration; Eye Security abused SQLite	Execution (Eye Security chain)

CVE	Severity	Description	Role in chains
		`load_extension()` to load a native library [6][9]	
CVE-2026-129242	8.6	Deserialization in JDBC user/role services; an attacker-supplied HSQLDB database triggers deserialization [8][10]	Execution (maintainer/CryptoCat chain)

All six are fixed in GeoServer 2.27.7, 2.28.6, and 3.0.2 [3][4][5][15]. CVE-2026-120705 also requires the GeoTools `gt-metadata` library to be at 33.7, 34.6, or 35.2 [3]. Organizations that build GeoServer from source or embed GeoTools in other applications need to confirm both components. Eye Security also notes that the 2.27.x branch is no longer officially supported, so organizations on that line should plan to move to a supported series rather than depend on further backports [9].

How the Chains Work

Two chains have been published, and they share the same core. In the Eye Security chain, the attacker uses the CVE-2026-120705 XInclude file read to retrieve `users.xml`, which holds GeoServer usernames and password digests. The attacker also retrieves `security/config.xml`, which holds the remember-me signing key [9]. Using CVE-2026-129245, they then combine the key and the stored password representation to forge a valid administrator remember-me cookie. Eye Security describes this as effectively pass-the-hash, because the plaintext password is never needed [9]. With administrator access, the attacker configures a JDBC security service that loads a native library through SQLite, achieving code execution on both Linux and Windows deployments (CVE-2026-120704) [9].

The second chain, documented by the GeoServer maintainers and by CryptoCat, adds two steps at the start that make it more dependable in default configurations [5][10]. CVE-2026-129244 first leaks the data directory path, so the attacker knows exactly which files to request. CVE-2026-129243 then lets the attacker get past the admin-only rule protecting stored queries by addressing the service as `x/WFS` rather than `WFS`. In CryptoCat's description, GeoServer then turns escaped text in a saved stored query into live XInclude elements. This leaks the remember-me key and the administrator digest, and the attacker forges the cookie as in the first chain [1][10]. The final step points a JDBC user service at an uploaded HSQLDB database whose bundled driver deserializes a stored value, which leads to command execution (CVE-2026-129242) [10].

One finding in the maintainers' advisory should shape how defenders think about remediation. The advisory states that an attacker who obtains an administrator password digest can log in, through any file disclosure or a copy of the data directory. It adds that changing the key in `security/config.xml` does not help when the same file disclosure also reveals the key [5]. Rotating the key is therefore not a meaningful compensating control on an unpatched server. After the upgrade, the remember-me key is no longer stored in the data directory: each node generates a random key, and existing cookies are invalidated. Clusters supply a shared key through the `GEOSERVER_REMEMBERME_KEY` application property [5].

Observed Exploitation and the CVE Attribution Question

watchTowr reported in-the-wild exploitation against its global honeypot network early on November 25, 2026. It observed actors from multiple IP addresses validating vulnerable systems with error-based probes that created stored queries, confirmed they existed, and then deleted them [1]. The behavior points to large-scale validation of targets, which typically comes before follow-on exploitation, rather than to a single targeted operation. watchTowr's Yordan Ganchev advised that any exposed system be audited for credential leakage, unauthorized access, and code execution on the host [1].

There is one discrepancy in the public record that defenders should be aware of. The Hacker News article's headline, the CISA KEV listing, and CryptoCat's summary all name CVE-2026-120705 and CVE-2026-129243 as the exploited pair [1][2][10]. However, the Hacker News quotes Ganchev as saying the observed activity leveraged CVE-2026-120705 and CVE-2026-129244 [1]. We were unable to review watchTowr's original post to resolve this. Both readings are plausible: creating stored queries anonymously requires the CVE-2026-129243 bypass, while error-based probing fits the CVE-2026-129244 path-disclosure behavior. The practical implication is unchanged. All six CVEs are fixed in the same releases, and the observed probes are consistent with the opening stages of the full chain.

The KEV deadline was also unusually short. The KEV catalog entries set a November 30, 2026 due date, three days after the November 27 listing, under BOD 26-04 [16][21], and the Hacker News reports the same date [1]. CISA's November 27 alert names the vulnerabilities but does not state the due date in its text [2]. Organizations outside the federal mandate can reasonably read the compressed timeline as a signal of CISA's assessed urgency rather than as a compliance date that does not apply to them.

WeaveLotus: GeoServer as an Espionage Foothold

On November 27, 2026, SOCRadar published research on a previously undocumented intrusion set it calls WeaveLotus, operating a campaign it names RedOps [11][12]. According to the Hacker News's account of that research, the activity took place in August and September 2026. It comprised five

confirmed intrusions, three in Thailand and two in the Philippines, plus reconnaissance against more than 30 Indonesian organizations that did not progress further. Targets were military, government, and legislative organizations, with an apparent focus on South China Sea defense and military agreements [11]. SOCRadar stated that initial access came primarily from exploiting web application vulnerabilities and default credentials in open-source software, including GeoServer, JasperReports, osTicket, and exposed Laravel debug-mode configurations. The actor then kept persistent access through reverse SSH tunnels and moved laterally into downstream networks [11].

The GeoServer intrusion in this campaign hit a Thai military organization. The Hacker News reports that initial access was likely achieved through CVE-2024-36401, not the November 2026 flaws [11]. After that, the actor deployed a SOCKS5 proxy and a reverse SSH tunnel, enumerated and downloaded records through an unauthenticated Directus CMS API, and ran OCR on harvested images to extract English and Thai text [11]. Other intrusions in the campaign relied on a JasperReports server with its default `jasperadmin` credentials and on a known unauthenticated osTicket SQL injection (CVE-2021-42235) [11]. The Hacker News characterized the group as Vietnam-sponsored. SOCRadar's own wording is more cautious: the evidence, which includes Vietnamese-language code comments, UTC+07:00 working hours, and target selection, supports tracking WeaveLotus as a distinct cluster "without conclusively establishing state sponsorship" [11]. We were unable to retrieve the SOCRadar report directly, so these details rely on the Hacker News's summary.

WeaveLotus matters here less for its attribution than for what it shows about exploitation economics. The actor did not need zero-days. According to SOCRadar's findings as summarized by the Hacker News, a GeoServer vulnerability on the KEV list for more than two years (likely CVE-2024-36401), a reporting server with factory credentials, and a 2021 osTicket flaw were sufficient to compromise military and government organizations [11]. At least one espionage-oriented actor is therefore exploiting older, unpatched GeoServer deployments. The November 2026 chains, which need no credentials, are plausible additions to such toolkits.

Why Geospatial Servers Keep Getting Hit

In CSA's assessment, several structural factors may explain why GeoServer keeps appearing in exploitation reporting. First, it is internet-exposed by design: OGC services exist so that external clients can consume them, anonymous WFS access is a common configuration, and Eye Security alone identified more than 3,000 internet-accessible instances [9]. Second, ownership is often unclear. GIS platforms are frequently installed by analysts, researchers, or contractors and may not appear in the CMDB or vulnerability scanner scope used by central security teams. Third, the data directory concentrates high-value secrets, including password digests, signing keys, and database connection strings for PostGIS and other back ends. As a result, a file-read bug can lead to full administrative compromise, an impact that

the base CVSS score for a disclosure flaw may not capture. Finally, geospatial servers increasingly sit in data and AI analytics pipelines, feeding imagery, sensor, and location data into models and dashboards. A compromise can therefore become a path to the data stores behind the map layers, and potentially a way to tamper with data that downstream analytics trust.

Recommendations

Immediate Actions

The first priority is to find every GeoServer instance, including those outside central IT's inventory. Search external attack-surface data, internal scanner results, and container registries for GeoServer images. Check each instance's version under About GeoServer > Build Information [9]. Upgrade every instance to 2.27.7, 2.28.6, or 3.0.2 or later, and confirm that the GeoTools components meet the minimum versions listed in the CVE-2026-120705 advisory [3][15]. Federal civilian agencies subject to BOD 26-04 face the November 30, 2026 KEV deadline [16][21].

Where an upgrade cannot be completed immediately, the maintainers' advisories describe three interim measures that reduce exposure without removing it. These measures should be applied together and treated as temporary:

- Restrict or disable WFS for anonymous users through service security, or disable WFS entirely if it is not needed [3].
- At a reverse proxy or WAF, block any `service` parameter containing `/`, whether it appears in the query string or in the XML request body [4].
- Remove `rememberme` from the `web` filter chain [5].

Beyond the advisories' measures, removing the instance from direct internet exposure where business requirements allow is a sensible general precaution [1].

After patching, carry out a compromise assessment on any instance that was internet-reachable while vulnerable. Following the advisories' guidance, inspect the `wfs/query` and `workspaces/*/wfs/query` endpoints for stored queries you did not create [4]. Review web and application logs for requests addressing prefixed service names such as `x/WFS` and for GetFeatureById requests containing XInclude content. Defenders should bear in mind that XInclude payloads may be escaped within stored-query definitions and that POST bodies are often not logged by default, so the absence of matches is not evidence of non-compromise. Check for unexpected JDBC user/role service configurations, uploaded SQLite or HSQLDB files, and new native libraries in the data directory. If

exposure cannot be ruled out, change administrator passwords as the advisory recommends [5]. Also rotate every credential stored in or reachable from the data directory, especially PostGIS and other data-store connection strings.

Short-Term Mitigations

Over the following weeks, organizations should bring GeoServer and similar geospatial services, such as GeoNetwork and map tile servers, into formal asset ownership and vulnerability management scope. Patch triggers should include upstream maintenance releases, not only published security advisories. The November 2026 timeline shows that fixes can ship weeks before disclosure, and exploitation can follow disclosure within a day [1][9]. Put administrative interfaces behind an identity-aware proxy or VPN so that they are not reachable from the internet. Run GeoServer under a dedicated low-privilege service account. Also limit the database privileges of data-store accounts, since escalation paths such as CVE-2026-76904 become more dangerous when the back-end PostgreSQL account has superuser or program-execution rights [14].

Organizations should also review default credentials and patch levels across the wider open-source estate that WeaveLotus targeted. SOCRadar reports that JasperReports (default credentials), osTicket (CVE-2021-42235), exposed Laravel debug configurations, and a legacy Keycloak 3.4 server whose credential store was dumped and cracked all featured in the campaign [11]. These platforms deserve the same inventory and hardening attention as GeoServer. Egress filtering on GeoServer hosts can limit both the SSRF component of CVE-2026-120705 and the reverse SSH tunneling that WeaveLotus relied on for persistence [3][11].

Strategic Considerations

The recurring GeoServer exploitation pattern is a specific case of a broader problem: specialist open-source infrastructure that sits outside mainstream patch programs while staying exposed to the internet. Security leaders should consider an "unowned infrastructure" review. Its goal would be to identify platforms installed by research, analytics, or operational teams that hold sensitive data or credentials but lack a named security owner. Where geospatial data feeds AI or analytics pipelines, data-integrity controls should treat the GIS tier as a possible tampering point and not as a trusted source. As AI-assisted research continues to speed up discovery in mature open-source codebases [9], organizations should expect more chained disclosures of this kind. They should plan remediation capacity, including emergency change windows for non-traditional platforms, accordingly.

CSA Resource Alignment

CSA's July 2026 research note, CVE-2026-45659: SharePoint RCE Under Active Exploitation, is the closest precedent for this guidance [17]. That note argued that when an actively exploited flaw exposes cryptographic keys or credentials, rotation is part of remediation rather than optional hardening. The GeoServer chain illustrates the same point. Because CVE-2026-120705 discloses both the administrator digest and the remember-me key, any instance exposed while vulnerable should be handled as a credential-compromise incident, not simply as a missing patch.

The quiet window between the October fixes and the November disclosure, followed by exploitation within a day, illustrates the dynamics CSA analyzes in AI-Accelerated Vulnerability Discovery and the Patch Debt Crisis [18]. That paper describes how AI-assisted discovery increases vulnerability volume and shrinks exploitation windows faster than classical patch management can absorb. Eye Security's statement that its GeoServer chain was found with AI assistance is a concrete example [9]. CSA's The VulnOps Operating Model offers a practical response [19]. It proposes continuous vulnerability operations organized around remediation throughput. Using upstream maintenance releases as patch triggers, as recommended above, fits that model's emphasis on absorbing fixes continuously rather than reacting to advisories.

At the control level, the AI Controls Matrix (AICM) v1.1 provides the governance anchor [20]. Relevant controls in its Threat and Vulnerability Management (TVM) domain address vulnerability identification and remediation prioritization, which apply directly to known-exploited flaws. Its Application and Interface Security (AIS) domain addresses the secure configuration of exposed service interfaces such as OGC endpoints. Controls in its Identity and Access Management (IAM) domain address credential and session management, including default credentials and session-token integrity, both of which the GeoServer and WeaveLotus activity exploited. Organizations whose geospatial services feed AI or analytics pipelines should explicitly include those services in the scope of their AICM implementation.

References

[1] Lakshmanan, R. "Hackers Exploit Two GeoServer Flaws as Researchers Warn of Unauthenticated RCE Chains." The Hacker News, November 25, 2026 (updated).

[2] CISA. "CISA Adds Three Known Exploited Vulnerabilities to Catalog." Cybersecurity and Infrastructure Security Agency, November 27, 2026.

[3] GeoServer Project. "Unauthenticated WFS GetFeatureById XML injection (CVE-2026-120705), GHSA-39mw-5chv-jh47." GitHub Security Advisory, November 2026.

[4] GeoServer Project. "Service security rules bypassed with a prefixed service name such as x/WFS (CVE-2026-129243), GHSA-rv5g-g2r9-58rj." GitHub Security Advisory, November 2026.

[5] GeoServer Project. "Predictable remember-me key allows administrator session forgery (CVE-2026-129245), GHSA-hgm3-wq4h-8vvq." GitHub Security Advisory, November 2026.

[6] GeoServer Project. "CVE-2026-120704, GHSA-wc3v-48j7-xf57." GitHub Security Advisory, November 2026.

[7] GeoServer Project. "CVE-2026-129244, GHSA-4v26-c537-jvxc." GitHub Security Advisory, November 2026.

[8] GeoServer Project. "CVE-2026-129242, GHSA-9wf2-fcgq-vxhq." GitHub Security Advisory, November 2026.

[9] Teusink, N. "Unauthenticated remote code execution vulnerability in GeoServer." Eye Security, November 24, 2026.

[10] CryptoCat (J. Burgess). "GeoServer Pre-Authentication RCE via WFS and HSQLDB." cryptocat.me, November 2026.

[11] Lakshmanan, R. "Suspected Vietnam-Linked Hackers Target Southeast Asia in South China Sea Espionage Campaign." The Hacker News, November 27, 2026.

[12] SOCRadar. "RedOps: WeaveLotus Targets Southeast Asian Governments." SOCRadar, November 2026.

[13] NIST. "CVE-2024-36401 Detail." National Vulnerability Database, 2024.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.

[14] Lakshmanan, R. "GeoServer Zero-Day Targeted in Active Exploitation Attempts, Can Lead to RCE." The Hacker News, August 13, 2026.

[15] GeoServer Project. "GeoServer 3.0.2 Release." GitHub, 2026. See also 2.28.6 and 2.27.7.

[16] CISA. "Known Exploited Vulnerabilities Catalog." Cybersecurity and Infrastructure Security Agency, accessed November 29, 2026.

[17] Cloud Security Alliance. "CVE-2026-45659: SharePoint RCE Under Active Exploitation." CSA AI Safety Initiative, July 3, 2026.

[18] Cloud Security Alliance. "AI-Accelerated Vulnerability Discovery and the Patch Debt Crisis." CSA AI Safety Initiative, June 17, 2026.

[19] Cloud Security Alliance. "The VulnOps Operating Model." Cloud Security Alliance, 2026 (accessed November 29, 2026).

[20] Cloud Security Alliance. "AI Controls Matrix (AICM) v1.1." Cloud Security Alliance, accessed November 29, 2026.

[21] CISA. "BOD 26-04: Prioritizing Security Updates Based on Risk." Cybersecurity and Infrastructure Security Agency, 2026.

© 2026 Cloud Security Alliance. AI-assisted Rapid Research.