VORFALL-LAGEBILD

GitLab: kritische Lücke CVE-2026-97229 (CVSS 10) – jetzt patchen

Stand 28.10.2026 07:01 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Wer GitLab selbst betreibt, sollte heute prüfen, ob 19.4.2, 19.3.5 oder 19.2.8 läuft, und Server mit Internetzugang zuerst patchen.

2. Bei Maschinenbauern liegen in GitLab oft SPS-Projekte, Firmware-Builds und Fernwartungs-Zugangsdaten, deshalb gehört der Server ins Asset-Inventar und hinter ein VPN.

3. Bisher ist kein Angriff bestätigt. Der Exploit ist aber öffentlich, und die Schwester-Lücke wurde im September einen Tag nach dem Patch angegriffen.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
GitLab hat am 12.10.2026 kritische Patch-Releases für CE/EE veröffentlicht: 19.4.2, 19.3.5 und 19.2.8. Insgesamt sind es 24 Sicherheitsfixes (1 kritisch, 5 hoch, 14 mittel, 4 niedrig).	100 %	100 %	bestätigt
CVE-2026-97229 ist ein Integer-Overflow im CI/CD-Regex-Compiler. Laut GitLab kann ein nicht authentifizierter Nutzer „unter bestimmten Bedingungen“ über eine präparierte CI/CD-Konfiguration beliebigen Code auf dem Server ausführen. Bewertung: CVSS 3.1 = 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).	100 %	100 %	bestätigt
Betroffen sind 19.2 vor 19.2.8, 19.3 vor 19.3.5 und 19.4 vor 19.4.2. Version 19.3.4 hatte einen Bug bei Merge-Request-Seiten (Ona-Integration), den 19.3.5 behebt. 19.3.5 ist deshalb der richtige Stand.	100 %	100 %	bestätigt
Laut Rapid7 besteht der präparierte reguläre Ausdruck zunächst GitLabs Prüfung. Danach erzeugt Rubys Regex-Engine beim erneuten Kompilieren ungültige Instruktionen, und am Ende wird Code als Benutzer „git“ ausgeführt.	100 %	100 %	präzisiert
Rapid7 widerspricht der Einstufung „unauthentifiziert“ teilweise. Der Angreifer muss eine bösartige CI/CD-Konfiguration in einen Branch eines öffentlichen Projekts committen können. Wo sich jeder selbst registrieren und Projekte anlegen kann, fällt diese Hürde praktisch weg.	100 %	100 %	präzisiert
Gemeldet hat die Lücke ein Forscher mit dem Handle „joaxcar“ über GitLabs HackerOne-Programm, also über ein Bug-Bounty-Programm und nicht wegen eines beobachteten Angriffs.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Im selben Release wurden weitere hohe Lücken geschlossen: CVE-2026-92883 (XSS, CVSS 8.7) und CVE-2026-16301 (fehlende Berechtigungsprüfung bei Downstream-Pipelines bzw. Pipelines auf geschützten Branches, CVSS 8.5).	100 %	100 %	bestätigt
Es handelt sich um einen gewöhnlichen Programmierfehler, den ein Forscher gefunden und verantwortungsvoll gemeldet hat, nicht um eine gezielte Backdoor.	85 %	90 %	präzisiert
Auf typischen Firmen-Instanzen ohne öffentliche Registrierung greift die Einstufung „unauthentifiziert“ in der Praxis zu hoch, dort braucht ein Angreifer ein Konto.	70 %	60 %	offen
Bei erfolgreicher Ausnutzung kann ein Angreifer beliebigen Code auf dem GitLab-Server ausführen, und zwar als Benutzer „git“. Rapid7 hat das auf einem ungepatchten GitLab 19.4.1 CE nachgestellt. Gegen 19.4.2 funktionierte dieselbe Eingabe nicht.	100 %	100 %	bestätigt
Betroffen sind nur selbst gehostete Instanzen. GitLab.com ist gepatcht, Kunden von GitLab Dedicated müssen nichts tun.	100 %	100 %	bestätigt
Laut Rapid7 ist bisher keine Ausnutzung in freier Wildbahn bestätigt.	100 %	100 %	bestätigt
Laut CERT-EU ist unter den übrigen Fixes auch eine Cache-Poisoning-Lücke (CVSS 8.2), über die geschützte CI/CD-Variablen offengelegt werden könnten.	100 %	50 %	präzisiert
Für die Schwester-Lücke CVE-2026-85706 nennen Analysten als Folgen: Diebstahl von CI/CD-Variablen, Runner-Tokens, SSH- und Deploy-Keys, kompromittierte Pipelines und Lateral Movement auf weitere Systeme.	100 %	70 %	präzisiert
Nach einer erfolgreichen RCE wären die Secrets auf dem Server (Quellcode, CI/CD-Variablen, Runner- und Deploy-Tokens, Keys) für den Angreifer erreichbar.	75 %	80 %	offen
Bei Herstellern, die Firmware oder Software über GitLab-Pipelines bauen, bestünde das Risiko manipulierter Builds vor der Auslieferung an Kunden (Supply Chain).	40 %	35 %	offen
Das Update enthält Datenbank- bzw. Post-Deploy-Migrationen. Single-Node-Instanzen haben beim Upgrade eine Downtime, Multi-Node-Instanzen lassen sich ohne Downtime aktualisieren.	100 %	100 %	bestätigt

Frühere Aussage	vorher	jetzt	Status
Rapid7 rät, außerhalb des normalen Zyklus zu patchen. Übergangsweise soll man anonymen Zugriff auf öffentliche Projekte einschränken und nicht vertrauenswürdigen Nutzern das Anlegen und Beschreiben öffentlicher Projekte verbieten. Das blockiert nur den gezeigten Weg und ersetzt den Patch nicht.	100 %	100 %	präzisiert
Bei der Schwester-Lücke wurde empfohlen, Deploy-Tokens, CI-Variablen und SSH-Keys zu rotieren und die Logs zu durchsuchen.	100 %	70 %	offen
We… (Aussage im Auftrag abgeschnitten, nicht bewertbar)	unbekannt %	45 %	offen

Neu seit dem letzten Stand

• Rapid7 hat am 13.10. einen Proof of Concept auf GitHub veröffentlicht. Er funktioniert zuverlässig auf dem offiziellen 19.4.1-CE-Image (amd64), braucht aber viel Speicher.

• Censys zählt 25.766 verwundbare Hosts, Deutschland liegt mit 6.469 vorn. EPSS 18,4 %.

• In der technischen Analyse vom 16.10. sagt Rapid7: Nur der letzte Schritt läuft ohne Anmeldung, den von GitLab gemeinten Weg ganz ohne Konto kennt Rapid7 nicht.

• Ruby hat am 23.10. die Onigmo-Fehler behoben (4.0.9, 3.4.12, 3.3.13). Zur Familie gehören vier GitLab-CVEs, darunter CVE-2026-110264 mit CVSS 10.0.

• GitLab hat sechs Threat-Detections veröffentlicht. Rapid7 nennt Log-Indizien (CI-Lint mit HTTP 502, Abstürze von Puma-Workern).

• Bis zum letzten auffindbaren Stand (26.10.) ist weiter keine Ausnutzung bestätigt und kein KEV-Eintrag vorhanden.

• Abweichung bei den Quellen: CERT-EU und SOC Prime nennen 19.3.4 als Fix, GitLab selbst nennt 19.3.5. Maßgeblich ist GitLab.

• Abweichung bei den Quellen: CERT-EU beschreibt eine Cache-Poisoning-Lücke mit CVSS 8.2. In GitLabs Tabelle hat Cache Poisoning (CVE-2026-100755) aber CVSS 4.6, und der Wert 8.2 gehört zu CVE-2026-14814 (Repository-Dateizugriff).

Wissensstand



■ Wissen 46 % ■ Wahrscheinlich 26 % ■ Nicht bekannt 28 %

Technik, Versionen und Patch sind durch GitLab und Rapid7 gut belegt. Ob angegriffen wird, wie die Lücke ganz ohne Konto ausgenutzt werden kann und welche Folgen sich bei echten Betreibern zeigen, ist dagegen offen. Die Host-Zahlen stammen von Censys und sind nur aus zweiter Hand (Fachpresse) überliefert.

1. Was ist passiert, und warum?

WISSEN

• GitLab hat am 12.10.2026 die Patch-Releases 19.4.2, 19.3.5 und 19.2.8 für CE/EE veröffentlicht. Sie enthalten 24 Sicherheitsfixes, davon 1 kritisch, 5 hoch, 14 mittel und 4 niedrig. (100 %) [https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

• CVE-2026-97229 ist ein Integer-Overflow im CI/CD-Regex-Compiler. Laut GitLab kann ein nicht authentifizierter Nutzer „unter bestimmten Bedingungen“ Code auf dem Server ausführen. CVSS 10.0. (100 %) [https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

• Die Ursache liegt in Rubys Regex-Engine Onigmo. Am 23.10.2026 hat Ruby die Versionen 4.0.9, 3.4.12 und 3.3.13 mit Fixes für vier Onigmo-Fehler veröffentlicht, darunter den Fehler hinter CVE-2026-97229. (100 %) [https://securityonline.info/ruby-security-update-onigmo-gitlab-cves]

• Rapid7 zufolge muss ein Angreifer im gezeigten Weg eine bösartige CI-Konfiguration in ein öffentliches Projekt pushen können, also Schreibrechte haben. Nur die letzte Anfrage läuft ohne Anmeldung. Wie der ursprünglich gemeldete Angriff ohne diese Voraussetzung auskommt, weiß Rapid7 nach eigener Aussage noch nicht. (100 %)
[https://www.rapid7.com/blog/post/ra-gitlab-ci-cd-regex-integer-overflow-technical-analysis-cve-2026-97229/]

• Gemeldet hat die Lücke der Forscher „joaxcar“ über GitLabs HackerOne-Programm. (100 %)
[https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

NICHT BEKANNT
• Mit welchem Weg die Lücke laut GitLab ganz ohne Konto ausnutzbar ist

• Ob andere Ruby-Anwendungen außerhalb von GitLab über denselben Onigmo-Fehler angreifbar sind

WAHRSCHEINLICH (Einschätzung)
• Die Lücke ist ein gewöhnlicher Programmierfehler in der Regex-Engine und keine absichtlich eingebaute Backdoor. (90 %) – Bug-Bounty-Meldung, vier verwandte Onigmo-Fehler mit offiziellem Ruby-Fix, Fehlerklasse Integer-Overflow (CWE-190).

• Auf Firmen-Instanzen ohne Selbstregistrierung und ohne öffentliche Projekte braucht ein Angreifer in der Praxis ein Konto. (60 %) – So beschreibt Rapid7 den nachgestellten Weg. GitLab bleibt aber bei PR:N und Rapid7 räumt ein, den ursprünglichen Weg nicht zu kennen.

2. Was ist die Auswirkung?

WISSEN
• Rapid7 hat auf GitLab 19.4.1 CE die Ausführung von Befehlen als Benutzer „git“ nachgestellt. Gegen 19.4.2 funktionierte das nicht. (100 %)
[https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/]

• Rapid7 hat am 13.10. einen Proof of Concept auf GitHub veröffentlicht. (100 %)
[https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/]

• Betroffen sind nur selbst gehostete Instanzen. GitLab.com ist gepatcht, Dedicated wurde vorab intern gepatcht. (100 %) [https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

• Eine Ausnutzung in freier Wildbahn ist nicht bestätigt (Rapid7, Stand letzter Aktualisierung 16.10.), ebenso wenig ein KEV-Eintrag. (100 %)
[https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/]

• Der EPSS-Wert (Wahrscheinlichkeit einer Ausnutzung in 30 Tagen) lag laut Bericht bei 18,4 %. (100 %) [https://securityonline.info/gitlab-rce-cve-2026-97229-poc-disclosed/]

NICHT BEKANNT
• Ob es tatsächlich kompromittierte Server gibt

• Ob Daten oder Secrets abgeflossen sind

• Ob Firmware- oder Software-Builds irgendwo manipuliert wurden

WAHRSCHEINLICH (Einschätzung)
• Wer Code als „git“ ausführt, erreicht Repositorys, CI/CD-Variablen und Tokens der Instanz. (80 %) – Unter „git“ laufen die GitLab-Anwendungsprozesse. Rapid7 dokumentiert die genaue Reichweite aber nicht.

• Bei Herstellern mit Firmware-Builds über GitLab bestünde das Risiko manipulierter Auslieferungen (Supply Chain). (35 %) – Technisch denkbar, braucht aber zusätzliche Schritte. Kein solcher Fall ist belegt.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN
• Das Update enthält Datenbank-Migrationen. Single-Node-Instanzen haben eine Downtime, Multi-Node-Instanzen lassen sich ohne Downtime aktualisieren. (100 %)
[https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

• GitLab hat sechs Threat-Detections für selbst gehostete Instanzen veröffentlicht. (100 %)
[https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

• Übergangsweise rät Rapid7, anonymen Zugriff auf öffentliche Projekte einzuschränken, nicht vertrauenswürdigen Nutzern das Beschreiben öffentlicher Projekte zu verbieten oder die CI-Lint-Route zu sperren. Das ersetzt den Patch nicht. (100 %)
[https://www.rapid7.com/blog/post/ra-gitlab-ci-cd-regex-integer-overflow-technical-analysis-cve-2026-97229/]

• Als Indizien in Logs nennt Rapid7 auffällig langsame CI-Lint-Anfragen mit HTTP 502, Abstürze von Puma-Workern und plötzliche Speichersprünge. (100 %)
[https://www.rapid7.com/blog/post/ra-gitlab-ci-cd-regex-integer-overflow-technical-analysis-cve-2026-97229/]

NICHT BEKANNT
• Dauer einer Bereinigung im Ernstfall. Es gibt keinen bekannten Vorfall, an dem man das messen könnte

WAHRSCHEINLICH (Einschätzung)
• Ein Patch dauert typischerweise Stunden. Ist ein Server kompromittiert, dauert es Tage bis Wochen, weil alle Tokens, Keys und CI-Variablen rotiert werden müssen. (70 %) – Erfahrungswerte aus früheren GitLab-Vorfällen und der Incident Response bei CI/CD-Systemen. Für diese CVE nicht belegt.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN
• Die Lücke betrifft den GitLab-Server, also IT. Es gibt keine Meldung über Folgen in Produktionsanlagen. (100 %) [https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-2-released/]

NICHT BEKANNT
• Wie viele Maschinenbauer oder Betreiber SPS-Projekte und Firmware-Builds in betroffenen GitLab-Instanzen haben

WAHRSCHEINLICH (Einschätzung)
• Eine direkte physische Beschädigung von Anlagen durch diese Lücke ist sehr unwahrscheinlich. (10 %) – Dazu wären mehrere weitere Schritte über Build-Pipeline, Auslieferung und Aufspielen in der Anlage nötig.

• Der realistischere OT-Schaden sind abgeflossene SPS-Projekte, Anlagendokumentation und Fernwartungs-Zugangsdaten. Sie können spätere Angriffe erleichtern. (45 %) – In Entwicklungs-Repositorys liegen solche Daten häufig, ihr Abfluss wäre eine Vorstufe. Für diese CVE ist kein Fall belegt.

5. Wie viele solcher Ziele gibt es?

WISSEN
• Laut Censys laufen rund 25.766 internet-erreichbare Hosts und 79.224 Webauftritte mit verwundbaren Versionen. 31 % von 82.454 erkannten GitLab-Hosts sind ungepatcht. (100 %)
[https://securityonline.info/gitlab-rce-cve-2026-97229-poc-disclosed/]

• Deutschland liegt mit 6.469 verwundbaren Hosts vorn, vor Russland (4.173) und den USA (2.927). So berichtet es die Fachpresse unter Berufung auf Censys. (100 %)
[https://securityonline.info/gitlab-rce-cve-2026-97229-poc-disclosed/]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Deutschland: 148369 gesamt (DNP3 34441, OMRON FINS 25856, ProConOS 17136, EtherNet/IP 16235, Siemens S7 8060, OPC UA 5613) (100 %)

NICHT BEKANNT
• Censys-Originalbericht nicht gefunden, Zahlen nur aus zweiter Hand

• Wie viele der Hosts Selbstregistrierung oder öffentliche Projekte erlauben und damit dem gezeigten Weg offenstehen

• Wie viele davon zu Industrie oder Maschinenbau gehören

• Aktueller Stand nach dem 14.10.

WAHRSCHEINLICH (Einschätzung)
• Die Zahl der ungepatchten Hosts ist seit Mitte Oktober gesunken, ein Teil bleibt aber dauerhaft offen. (75 %) – Typischer Patch-Verlauf. 2021 war bei CVE-2021-22205 ein halbes Jahr nach dem Patch noch etwa die Hälfte ungepatcht.

6. Kann das wieder passieren?

WISSEN

• Die Schwester-Lücke CVE-2026-85706 (CVSS 10.0, Path Traversal) wurde am 10.09.2026 gepatcht und am 11.09.2026 in den CISA-KEV aufgenommen. (100 %)
[https://www.cisa.gov/news-events/alerts/2026/09/11/cisa-adds-one-known-exploited-vulnerability-catalog]

• Laut CISA wurden seit 2021 mindestens fünf GitLab-Schwachstellen in Angriffen ausgenutzt. (100 %) [https://www.cybersecuritydive.com/news/gitlab-vulnerability-remote-code-execution/832736/]

• 2021 machten Angreifer über CVE-2021-22205 Tausende ungepatchte GitLab-Server zu einem DDoS-Botnet mit über 1 Tbps. (100 %) [https://www.helpnetsecurity.com/2021/11/04/cve-2021-22205/]

NICHT BEKANNT

• Ob CVE-2026-97229 noch in den KEV kommt

WAHRSCHEINLICH (Einschätzung)

• CVE-2026-97229 wird in den nächsten Wochen aktiv ausgenutzt. (45 %) – Für eine Ausnutzung sprechen der öffentliche PoC und die vielen offenen Hosts. Dagegen sprechen die Vorbedingung Schreibrechte, der hohe Speicherbedarf und die zielspezifischen Werte. Nach 16 Tagen ist noch nichts bestätigt.

• Es folgen weitere kritische GitLab-Lücken. (85 %) – Zwei Lücken mit CVSS 10 in zwei Monaten, dazu ein großes, attraktives Produkt.

Lage

GitLab hat am 12.10.2026 eine Schwachstelle mit CVSS 10.0 in selbst gehosteten CE/EE-Instanzen geschlossen. Ein präparierter regulärer Ausdruck in der CI/CD-Konfiguration kann dort zur Codeausführung als Benutzer „git“ führen. Rapid7 hat seit dem 13.10. einen Proof of Concept öffentlich, Censys zählt rund 25.766 verwundbare Hosts im Internet, die meisten davon in Deutschland. Eine Ausnutzung in freier Wildbahn ist nach allen auffindbaren Quellen (Stand bis 26.10.) nicht bestätigt, und die Lücke steht nicht im CISA-KEV.

Angriff	Kein bestätigter Angriff. Es gibt eine kritische RCE-Schwachstelle in selbst gehostetem GitLab mit öffentlichem PoC.
Wann / Status	Patch 12.10.2026, PoC 13.10.2026 · unklar
Täter	keine bekannt – unbekannt
Betreiber / Branche	Betreiber selbst gehosteter GitLab-Instanzen (Produkt von GitLab Inc.) · branchenübergreifend, Softwareentwicklung
Anlage / Alter	IT-Entwicklungsplattform (Quellcode, CI/CD) · Versionen 19.2 bis 19.4
Region	weltweit, Schwerpunkt verwundbarer Hosts in Deutschland
Auswirkungen	Keine Auswirkungen auf Versorgung oder Bevölkerung bekannt. Das Risiko betrifft Entwicklungs- und Build-Umgebungen von Unternehmen.
Behörden	CERT-EU (Advisory 2026-016). Eine Warnung von BSI oder CERT-Bund wurde in der Recherche nicht gefunden, das sollte man direkt auf bsi.bund.de prüfen. CISA: kein KEV-Eintrag für CVE-2026-97229.
Regulatorik	Wird ein Vorfall bei NIS2-pflichtigen Einrichtungen erheblich, gilt die Meldepflicht an das BSI (Frühwarnung binnen 24 h). Für Hersteller mit Produkten mit digitalen Elementen gelten ab 11.09.2026 die CRA-Meldepflichten für aktiv ausgenutzte Schwachstellen in eigenen Produkten. Ob ein kompromittierter Build-Server darunter fällt, ist eine Einzelfallfrage. Patchen ohne Vorfall löst keine Meldepflicht aus.

Angriffsvektor

Bekannt: Präparierte CI/CD-Konfiguration mit manipuliertem regulärem Ausdruck in einem öffentlichen Projekt, ausgelöst über die CI-Lint-Funktion (laut Rapid7). Den vollständigen Weg

ohne Konto hat GitLab nicht veröffentlicht.

• Selbstregistrierung auf öffentlich erreichbarer Instanz, danach eigenes öffentliches Projekt anlegen (hoch): Genau dieser Weg wurde nachgestellt. Viele Instanzen lassen Registrierung offen.

• Kompromittiertes Konto von Mitarbeitern oder Dienstleistern (Phishing, Credential Stuffing) (mittel): Typischer Erstzugang. Bei Maschinenbauern haben oft auch externe Integratoren Konten.

• Unbekannter Weg ganz ohne Konto, wie ihn GitLabs CVSS-Bewertung nahelegt (gering): GitLab bewertet PR:N, öffentlich ist dieser Weg aber nicht beschrieben.

Zeitleiste

10.09.2026 GitLab patcht die Schwester-Lücke CVE-2026-85706 – bestätigt [https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-3-2-released/]

11.09.2026 CISA nimmt CVE-2026-85706 in den KEV auf – bestätigt [https://www.cisa.gov/news-events/alerts/2026/09/11/cisa-adds-one-known-exploited-vulnerability-catalog]

12.10.2026 GitLab veröffentlicht 19.4.2, 19.3.5 und 19.2.8. Am selben Tag erscheint das CERT-EU Advisory 2026-016 – bestätigt [https://cert.europa.eu/publications/security-advisories/2026-016/]

13.10.2026 Rapid7 veröffentlicht Advisory und PoC – bestätigt [https://www.rapid7.com/blog/post/etr-cve-2026-97229-critical-unauthenticated-remote-code-execution-in-gitlab/]

14.10.2026 Censys-Zahlen: 25.766 verwundbare Hosts, Deutschland vorn – berichtet [https://securityonline.info/gitlab-rce-cve-2026-97229-poc-disclosed/]

16.10.2026 Rapid7 veröffentlicht die technische Analyse, weiterhin ohne bestätigte Ausnutzung – bestätigt [https://www.rapid7.com/blog/post/ra-gitlab-ci-cd-regex-integer-overflow-technical-analysis-cve-2026-97229/]

23.10.2026 Ruby veröffentlicht Fixes für die Onigmo-Engine (4.0.9, 3.4.12, 3.3.13) – berichtet [https://securityonline.info/ruby-security-update-onigmo-gitlab-cves]

Vergleichsfälle

• CVE-2026-85706 GitLab Path Traversal (2026): Einen Tag nach dem Patch stand die Lücke im KEV, das Zeitfenster zum Patchen ist also sehr kurz. [https://www.theregister.com/security/2026/09/14/perfect-10-gitlab-bug-under-attack-days-after-patch-lands/5296176]

• CVE-2021-22205 GitLab ExifTool (2021): Monate nach dem Patch war etwa die Hälfte der Server noch offen und wurde zum Botnet. [https://www.helpnetsecurity.com/2021/11/04/cve-2021-22205/]

• CVE-2023-7028 GitLab Account Takeover (2024): Vom Patch im Januar bis zum KEV-Eintrag im Mai vergingen Monate, eine Ausnutzung kann also auch spät kommen. [https://scmagazine.com/news/critical-gitlab-account-takeover-flaw-added-to-cisas-kev-catalog]

Begriffe einfach erklärt

GitLab: Eine Plattform, auf der Firmen Programmcode speichern und automatisch zu fertiger Software bauen lassen.

CI/CD-Pipeline: Ein automatischer Ablauf, der aus Code fertige Software oder Firmware baut und ausliefert.

RCE (Remote Code Execution): Ein Angreifer kann aus der Ferne eigene Befehle auf einem fremden Server ausführen.

Proof of Concept (PoC): Ein öffentlich verfügbares Beispielprogramm, das zeigt, dass ein Angriff funktioniert.

CVSS 10.0: Die höchste Stufe auf der Skala, mit der Schwachstellen nach Schwere bewertet werden.

KEV-Katalog: Die Liste der US-Behörde CISA mit Schwachstellen, die nachweislich angegriffen werden.

OT: Die Technik, die Maschinen und Anlagen steuert, also das Gegenstück zur Büro-IT.

Früherer Stand: Erstmeldung (14.10.2026 08:26)

Wissen 43 % · wahrscheinlich 27 % · nicht bekannt 30 %

Am 12.10.2026 hat GitLab für selbst gehostete CE/EE-Instanzen die Versionen 19.4.2, 19.3.5 und 19.2.8 veröffentlicht. Damit ist CVE-2026-97229 geschlossen, ein Integer-Overflow im CI/CD-Regex-Compiler mit CVSS 10.0, über den Angreifer Code auf dem GitLab-Server ausführen können. Rapid7 hat die RCE nachgestellt und am 13.10. einen Proof of Concept verlinkt. In der Praxis braucht ein Angreifer laut Rapid7 ein Konto, mit dem er in ein öffentliches Projekt committen kann. Bis 13./14.10. ist keine Ausnutzung in freier Wildbahn bestätigt, die Lücke steht nicht im CISA-KEV, und ein konkreter Geschädigter ist nicht bekannt. Für Maschinenbauer und Hersteller ist der Fall heikel, weil dort in GitLab oft Quellcode, SPS-Projekte, Firmware-Build-Pipelines und CI/CD-Secrets liegen. Die Schwester-Lücke CVE-2026-85706 wurde im September etwa einen Tag nach dem Patch ausgenutzt.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.