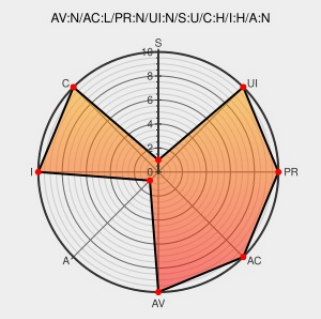
CVE-2022-1162

Published on: Not Yet Published

Last Modified on: 04/27/2022 08:35:00 PM UTC

CVE-2022-1162

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Gitlab from Gitlab contain the following vulnerability:

A hardcoded password was set for accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) in GitLab CE/EE versions 14.7 prior to 14.7.7, 14.8 prior to 14.8.5, and 14.9 prior to 14.9.2 allowing attackers to potentially take over accounts

CVE-2022-1162 has been assigned by cve@gitlab.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.9, <14.9.2**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.8, <14.8.5**

Affected Vendor/Software: **GitLab** - **GitLab** version **>=14.7, <14.7.7**

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
2022/CVE-2022-1162.json · master · GitLab.org / cves · GitLab	gitlab.com text/html	CONFIRM gitlab.com/gitlab-org/cves/-/blob/master/2022/CVE-2022-1162.json
Gitlab 14.9 Authentication Bypass ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/166828/Gitlab-14.9-Authentication-Bypass.html
Not Found	gitlab.com text/html Inactive Link Not Archived	MISC gitlab.com/gitlab-org/gitlab/-/issues/357210

Related QID Numbers

376517 GitLab Static Password Vulnerability For Accounts Registered Using OmniAuth

690828 Free Berkeley Software Distribution (FreeBSD) Security Update for gitlab (8657eedd-b423-11ec-9559-001b217b3468)

730422 GitLab Static Password Vulnerability For Accounts Registered Using OmniAuth

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gitlab	Gitlab	All	All	All	All
Application	Gitlab	Gitlab	All	All	All	All

cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*:

cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:*:

Discovery Credit

This vulnerability has been discovered internally by the GitLab team

Social Mentions

Source	Title	Posted (UTC)
@QuellaGala	What's the passwd?+_+ #GitLab Critical Security Release: 14.9.2, 14.8.5, and 14.7.7 CVE-2022-1162 Static passwords… twitter.com/i/web/status/1…	2022-04-01 03:35:47
@miglen	@exceptionalnull @gitlab Nope, it's this vulnerability CVE-2022-1162: about.gitlab.com/releases/2022/… Basically, they had… twitter.com/i/web/status/1…	2022-04-01 06:34:51
@d0znpp	CVE-2022-1162 Gitlab hardcoded password allows to bypass Oauth, saml, and ldap while OmniAuth enabled. Try passwor… twitter.com/i/web/status/1…	2022-04-01 10:30:11
@autumn_good_35	CVE-2022-1162 はcritical。 GitLab .comの方は対処したとのこと。 GitLab Critical Security Release: 14.9.2, 14.8.5, and 14.7.7… twitter.com/i/web/status/1…	2022-04-01 11:59:41
@gebutcher	Forwarded from LeakInfo CVE-2022-1162 В корректирующих обновлениях платформы для организации совместной разработки… twitter.com/i/web/status/1…	2022-04-01 12:06:03
@ando_Tw	『Gitlabにアカウントの乗っ取りを許す致命的な脆弱性』とする記事(CVE-2022-1162)	2022-04-01

@ando_fw	「Gitlabにアカウントの乗っ取りを許す致命的な脆弱性」という記事(CVE-2022-1162)。 twitter.com/BleepinCompute…	2022-04-01 15:07:35
@CKsTechNews	#Critical #Gitlab vulnerability lets attackers take over accounts CVE-2022-1162 Response about.gitlab.com/releases/2022/…	2022-04-01 15:31:31
@jbhall56	The bug (discovered internally and tracked as CVE-2022-1162) affects both GitLab Community Edition (CE) and Enterpr… twitter.com/i/web/status/1…	2022-04-01 16:55:50
@Cyb0Mancer	A critical vulnerability (CVE-2022-1162) that could allow hackers to take over user accounts using hardcoded passwo… twitter.com/i/web/status/1…	2022-04-01 17:15:38
@Th3PeKo	So for the #Gitlab CVE-2022-1162 with static creds even the committer was aware, that it's probably not acceptable… twitter.com/i/web/status/1…	2022-04-01 18:40:44
@Th3PeKo	My personal analysis thread on how the critical @gitlab CVE-2022-1162 was introduced. TL;DR; Code commit with "str… twitter.com/i/web/status/1…	2022-04-01 21:47:04
@foxbook	GitLabは、リモートの攻撃者がハードコードされたパスワードを使用してユーザーアカウントを乗っ取る可能性がある重大な重大度の脆弱性に対処しました。 このバグ（ CVE-2022-1162 ）は、GitLab Community… twitter.com/i/web/status/1…	2022-04-01 22:32:34
@foxbook	「GitLabは、これまでに侵害されたユーザーアカウントはないと述べていますが、同社は、自己管理型インスタンス管理者が CVE-2022-1162の影響を受ける可能性のあるユーザーアカウントを特定するために使用できるスクリプトを作… twitter.com/i/web/status/1…	2022-04-01 22:33:16
@TheHackersNews	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 04:04:58
@_DrFrusci	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 04:06:13
@IT_news_for_all	DevOps platform GitLab has released software updates to fix a critical vulnerability (CVE-2022-1162) that could all… twitter.com/i/web/status/1…	2022-04-02 04:07:01
@Swati_THN	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 04:27:00
@unix_root	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 06:27:00
@HackerGhosttube	DevOps platform GitLab has released software updates to fix a critical vulnerability (CVE-2022-1162) that could all… twitter.com/i/web/status/1…	2022-04-02 07:15:04
@eagerbeavertech	thehackernews.com/2022/04/gitlab… Tracked as CVE-2022-1162, the issue has a CVSS score of 9.1 and is said to have been di… twitter.com/i/web/status/1…	2022-04-02 08:03:23
@security_wang	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 08:27:00
@securityaffairs	Critical CVE-2022-1162 flaw in #GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297… #securityaffairs #hacking	2022-04-02 10:02:07
@Xc0resecurity	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts dlvr.it/SMqc4y	2022-04-02 10:03:02
@thedpsadvisors	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-02 10:03:03
@evanderburg	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts i.securitythinkingcap.com/SMqc6z	2022-04-02 10:03:04
@AcooEdi	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts dlvr.it/SMqc77 via securityaffairs	2022-04-02 10:03:04
@shah_sheikh	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts: GitLab has addressed a critical… twitter.com/i/web/status/1…	2022-04-02 10:03:04
@RedPacketSec	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts -	2022-04-02

	redpacketsecurity.com/critical-cve-2…… twitter.com/i/web/status/1…	10:03:12
@inayuta	侵害される可能性のあるユーザーを特定するスクリプトがリリース。 #gitlab #CVE-2022-1162 about.gitlab.com/releases/2022/…	2022-04-02 10:03:17
@iSecurity	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts isecurityfeed.wordpress.com/2022/04/02/cri…	2022-04-02 10:07:11
@IT_securitynews	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts itsecuritynews.info/critical-cve-2…	2022-04-02 10:10:07
@Alevskey	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts: ift.tt/VDOfqpM by Secur… twitter.com/i/web/status/1…	2022-04-02 10:10:09
@security_inside	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-02 10:12:40
@ciberconsejo	CVE-2022-1162 Critical GitLab vulnerability lets attackers take over accounts bleepingcomputer.com/news/security/…	2022-04-02 10:19:57
@daveDFIR	ift.tt/VDOfqpM .. Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts #news… twitter.com/i/web/status/1…	2022-04-02 10:28:29
@netsecu	securityaffairs.co/wordpress/1297… Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts #cybersecurity	2022-04-02 10:35:03
@cKure7	▰▰▰▰▱ Zero-Day: GitLab has addressed a critical vulnerability, tracked as CVE-2022-1162 (CVSS score of 9.1), that c… twitter.com/i/web/status/1…	2022-04-02 10:36:12
@greenhyhebe	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts ift.tt/VDOfqpM	2022-04-02 10:39:56
@profxeni	r/t "Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts" bit.ly/37679uU	2022-04-02 10:47:11
@ohhara_shiojiri	CVE-2022-1162	2022-04-02 10:51:14
@LudovicoLoreti	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297… #Security… twitter.com/i/web/status/1…	2022-04-02 11:09:50
@ScureInfosec	GitLab has addressed a critical vulnerability, tracked as CVE-2022-1162 (CVSS score of 9.1) The bug was address… twitter.com/i/web/status/1…	2022-04-02 11:44:40
@ipssignatures	The vuln CVE-2022-1162 has a tweet created 0 days ago and retweeted 10 times. twitter.com/Th3PeKo/status… #pow1rtrtwwcve	2022-04-02 12:06:01
@SecUnicorn	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts ift.tt/VDOfqpM #Infosec	2022-04-02 12:08:28
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-22965: 1.7M (audience size) CVE-2022-1162: 1.5M CVE-2022-2296… twitter.com/i/web/status/1…	2022-04-02 13:00:02
@YourAnonRiots	#DevOps platform GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could a… twitter.com/i/web/status/1…	2022-04-02 14:03:36
@Har_sia	CVE-2022-1162 har-sia.info/CVE-2022-1162.… #HarsiaInfo	2022-04-02 15:02:44
@0x009AD6_810	こちらの GitLab のアカウント乗っ取りが可能な脆弱性 CVE-2022-1162 bleepingcomputer.com/news/security/… 脆弱性報告者による経緯説明を読むといろいろと学ぶべきものがある	2022-04-02 16:13:15
@Whitehead4Jeff	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-02 17:52:25
@tony_cleal	securityaffairs.co/wordpress/1297…	2022-04-02 18:04:35

@Har_sia	CVE-2022-1162 har-sia.info/CVE-2022-1162.… #HarsiaInfo	2022-04-02 18:25:07
@SecurityNewsbot	Critical CVE-2022-1162 #flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297… #SecurityAffairs	2022-04-02 19:00:11
@Dinosn	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-02 19:15:49
@securityaffairs	Critical CVE-2022-1162 flaw in #GitLab allowed threat actors to take over accounts. securityaffairs.co/wordpress/1297… #securityaffairs #hacking	2022-04-02 20:10:24
@MariaRusanova88	The link: securityaffairs.co/wordpress/1297…	2022-04-02 20:21:26
@ntsuji	CVE-2022-1162 flaw in GitLab allowed threat actors to take over accountsSecurity Affairs securityaffairs.co/wordpress/1297…	2022-04-02 20:23:46
@foxbook	「GitLabの重大なCVE-2022-1162の欠陥により、脅威アクターがアカウントを乗っ取ることができました」 securityaffairs.co/wordpress/1297…	2022-04-02 21:07:50
@securezoo	GitLab issues security update for Critical hard-coded password vulnerability (CVE-2022-1162)… twitter.com/i/web/status/1…	2022-04-02 22:00:31
@ChiNetworks	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297… Via… twitter.com/i/web/status/1…	2022-04-02 23:57:47
@pjstevenson	GitLab has addressed a critical vulnerability, tracked as CVE-2022-1162 (CVSS score of 9.1), that could allow remot… twitter.com/i/web/status/1…	2022-04-03 02:39:46
@Secnewsbytes	CVE-2022-1162 flaw in GitLab allowed threat actors to take over accountsSecurity Affairs securityaffairs.co/wordpress/1297…	2022-04-03 07:40:51
@TechKeg	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…… twitter.com/i/web/status/1…	2022-04-03 08:41:32
@the_yellow_fall	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts securityonline.info/cve-2022-1162-… #opensource… twitter.com/i/web/status/1…	2022-04-03 09:22:56
@AcooEdi	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts dlvr.it/SMsyCL via securityo… twitter.com/i/web/status/1…	2022-04-03 09:27:04
@Dinosn	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts securityonline.info/cve-2022-1162-…	2022-04-03 10:11:56
@PentestingN	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts securityonline.info/cve-2022-1162-… CVE-2022-11… twitter.com/i/web/status/1…	2022-04-03 10:13:57
@securityaffairs	Critical CVE-2022-1162 flaw in #GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297… #securityaffairs #hacking	2022-04-03 12:43:52
@CVEtrends	Top 3 trending CVEs on Twitter Past 24 hrs: CVE-2022-1162: 714.2K (audience size) CVE-2022-22965: 509.3K CVE-2022-… twitter.com/i/web/status/1…	2022-04-03 13:00:03
@akaclandestine	O GitLab abordou uma vulnerabilidade crítica, rastreada como CVE-2022-1162 (pontuação CVSS de 9,1), que pode permit… twitter.com/i/web/status/1…	2022-04-03 13:56:36
@ipssignatures	The vuln CVE-2022-1162 has a tweet created 0 days ago and retweeted 11 times. twitter.com/0x009AD6_810/s… #pow1rtrtwwcve	2022-04-03 14:06:00
@Har_sia	CVE-2022-1162 har-sia.info/CVE-2022-1162.… #HarsiaInfo	2022-04-03 15:01:16
@stulda	Gitlab mám rád, ale těch bezpečnostních chyb je poslední dobou nějak moc. securityonline.info/cve-2022-1162-…	2022-04-03 15:58:20
@anonymousspide3	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts securityonline.info/cve-2022-1162-…	2022-04-03 17:51:25

@AWNetworks	Find recommendations for GitLab Password Security Vulnerability - CVE-2022-1162. ow.ly/EBHO50IzbvI	2022-04-03 18:00:42
@securityaffairs	Critical CVE-2022-1162 flaw in #GitLab allowed threat actors to take over accounts. securityaffairs.co/wordpress/1297… #securityaffairs #hacking	2022-04-03 20:56:05
@righthand_ai	GitLab has released software updates to address a critical security vulnerability that is tracked as CVE-2022-1162,… twitter.com/i/web/status/1…	2022-04-04 00:26:05
@MachinaRecord	⚠GitLabに重大な脆弱性（CVE-2022-1162）、脅威アクターによるアカウント乗っ取りが可能に ?TOTOLINK製品の新たな脆弱性、MiraiベースのDDoSキャンペーン「Beastmode」で使用される ?脆弱… twitter.com/i/web/status/1…	2022-04-04 02:28:51
@AP_Hofleitner	CVE-2022-1162: Gitlab flaw allows remote attackers to take over user accounts securityonline.info/cve-2022-1162-…	2022-04-04 02:29:03
@ipssignatures	The vuln CVE-2022-1162 has a tweet created 0 days ago and retweeted 13 times. twitter.com/Dinosn/status/… #pow1rtrtwwcve	2022-04-04 04:06:00
@M157q_News_RSS	GitLab修補允許駭客接管用戶帳號的重大漏洞 ithome.com.tw/news/150259 GitLab在3月31日釋出安全更新，主要是為了修補可被駭客接管帳號的CVE-2022-1162重大安全漏洞。	2022-04-04 07:31:14
@HiveWissen	#DevOps platform ##GitLab has released software updates to fix a critical #vulnerability (CVE-2022-1162) that could… twitter.com/i/web/status/1…	2022-04-04 08:02:17
@Kepa_Munoz	#GitLab has addressed a critical #vulnerability, tracked as CVE-2022-1162 (CVSS score of 9.1), that could allow rem… twitter.com/i/web/status/1…	2022-04-04 08:53:39
@237hackers	CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-04 09:25:09
@IT_news_for_all	GitLab устранил критическую уязвимость CVE-2022-1162, затрагивающую как GitLab Community Edition (CE), так и Enterp… twitter.com/i/web/status/1…	2022-04-04 10:35:05
@FrankMarano6	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts securityaffairs.co/wordpress/1297…	2022-04-04 12:45:11
@Har_sia	CVE-2022-1162 har-sia.info/CVE-2022-1162.… #HarsiaInfo	2022-04-04 15:01:21
@CVEreport	CVE-2022-1162 : A hardcoded password was set for accounts registered using an OmniAuth provider e.g. OAuth, LDAP,… twitter.com/i/web/status/1…	2022-04-04 20:08:14
@LinInfoSec	Gitlab - CVE-2022-1162: gitlab.com/gitlab-org/cve…	2022-04-04 23:01:46
/r/gitlab	Gitlab – Static passwords set during OmniAuth-based registration (CVE-2022-1162)	2022-04-01 09:14:47
/r/vulnintel	GitLab hardcoded password vulnerability allows to take over all accounts registered using an OmniAuth provider (e.g. OAuth, LDAP, SAML) CVE-2022-1162	2022-04-01 19:12:30
/r/InfoSecNews	Critical CVE-2022-1162 flaw in GitLab allowed threat actors to take over accounts	2022-04-02 11:45:37
/r/cyber1sec14all	Update your GitLab as soon as possible, your passwords are in danger	2022-04-04 17:38:03
/r/HowToHack	GitLab Releases Patch for Critical Vulnerability That Could Let Attackers Hijack Accounts. Tracked as CVE-2022-1162, the issue has a CVSS score of 9.1 and is said to have been discovered internally by the GitLab team.	2022-04-05 01:39:50
/r/KibernetinisSaugumas	"GitLab" kritinis pažeidžiamumas	2022-04-05 11:00:14

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report