Google Cloud

Notification details

[Action Required] Cloud Run jobs and worker pools losing root access due to a security update

11/21/25, 3:52 PM

Dear Google Cloud customer,

We're writing to let you know about an upcoming security update to Cloud Run jobs and worker pools that may result in a breaking change to your application.

Attacks similar to those disclosed in CVE-2025-31133, CVE-2025-52565, and CVE-2025-52881 allow an attacker to execute a full container breakout in your Cloud Run worker pools and jobs, leading to root privilege escalation out of the container into your sandboxed instance. A malicious actor with privileges to deploy a container image could exploit these vulnerabilities to gain access to your other containers within your Cloud Run sandboxed instance.

In order to close these vulnerabilities, containers running in Cloud Run will **no longer have true root access on the underlying execution environment.** See our public documentation to learn more about security restrictions that will apply to your container as a result of this change.

Please read on for more details about the impact of the security vulnerability, how to determine whether your application is compatible with the upcoming security update, and what to do if you determine that your application is not compatible.

What is happening

On January 5, 2026, we will begin rolling out the security update that will move Cloud Run jobs and worker pools to run inside a Linux user namespace and thus remove true root access by your container to the underlying execution environment. This will be a breaking change for applications that use Cloud Run in the following ways:

Mount a network file system in any way other than by using Cloud Run's fully-managed volume mounts feature. This includes running a mount process inside the container to mount any of the following: NFS, Cloud Filestore, SMB/CIFS, or any other network file system.

Use nested volume mounts - mounting a volume inside another volume.

Change the system time using adjtimex and adjtime syscalls.

Use sudo or other setuid binaries.

Use eBPF and other kernel-level security features.

Write to /proc/, /sys/, or other pseudo filesystems.

Use of other system calls or access system files that require root privileges on the Cloud Run instance's VM.

Affected projects

We have attached the list of affected projects to this notification.

We will apply these changes to all **Cloud Run worker pools and Cloud Run jobs** in these projects. Any Cloud Run services in these projects are already running inside a Linux user namespace.

What you need to do

1. **Determine whether any of these projects are incompatible with the security update.** We recommend that you review your Cloud Run jobs and worker pools in these projects and determine whether they perform any of the actions detailed above. Alternatively, you can test whether your containers are compatible with running inside a Linux user namespace by running your container inside a Linux user namespace locally or in a GCE VM using Docker's userns-remap feature or using rootless podman.

2. If necessary, **modify your containers before January 5, 2025** to make them compatible with running in a Linux user namespace. See our Security Restrictions documentation for more details. This may involve making the following changes:

   If you are using self-managed volume mounts, you will need to migrate to Cloud Run's fully managed volume mounts feature (NFS; Cloud Storage). This may involve migrating to NFS or Cloud Storage if you are currently using SMB, CIFS, 9P, or NBD.

   If you are not able to change your container to remove the need for true root access, we recommend moving your workload to GKE.

3. **Where possible, enable retries for your Cloud Run jobs.** This will help minimize disruption to your workloads in case additional jobs turn out to be incompatible with running in a Linux user namespace. In some cases, we may be able to proactively and temporarily exclude incompatible projects from the update.

4. **If you need more time** to make these changes, or if you would like the security update applied to your project earlier than January:

   Contact Google Cloud Support by creating a Support ticket under Cloud Run -> Develop and include reference issue number 462760403.

   We are able to grant extensions until March 31, 2026.

Timeline

January 5, 2026: Cloud Run will begin applying this security update to jobs and worker pools.

January 31, 2026: All Cloud Run jobs and worker pools will be running inside a user namespace unless you requested a temporary exemption.

March 31, 2026: All temporary exemptions expire and the security update will be applied to all Cloud Run containers.

Why we are making this change

On November 5, 2025, several security issues were disclosed in runc, an open source software component used for running containers. The attacks disclosed in these vulnerabilities (CVE-2025-31133, CVE-2025-52565, and CVE-2025-52881) allow an attacker to execute a full container breakout in Cloud Run worker pools and jobs, leading to root privilege escalation of the sandboxed instance running that container. An actor with privileges to deploy a malicious container image can exploit these vulnerabilities to gain access to other containers within the same Cloud Run instance.

We're here to help

We appreciate your business and apologize for any inconvenience this may have caused. If you have any questions or require assistance, please contact Google Cloud Support by creating a Support ticket under Cloud Run -> Develop and include reference issue number 462760403.

Sincerely,

Google Cloud Support

Reference: 462760403

attachment.csv