Security Health Analytics findings

Security Health Analytics scanners generate vulnerability finding types that are available in Security Command Center.

Scanners and findings

The following tables describe the scanner types and specific vulnerability finding types that Security Health Analytics can generate. You can filter findings by scanner name and finding type using the Security Command Center Vulnerabilities tab in the Google Cloud Console.

2-Step verification findings

The `2SV_SCANNER` detects vulnerabilities related to 2-step verification for users.

Table 1. 2-Step verification scanner

Category	Finding description
`2SV_NOT_ENFORCED`	Indicates that there are users who aren't using 2-step verification.

API key vulnerability findings

The `API_KEY_SCANNER` scanner detects vulnerabilities related to API keys used in your cloud deployment.

Table 2. API key scanner

Category	Finding description
`API_KEY_APIS_UNRESTRICTED`	Indicates that there are API keys being used too broadly, and should be limited to allow only the APIs needed by the application.

`API_KEY_APPS_UNRESTRICTED`	Indicates that there are API keys being used in an unrestricted way, allowing use by any untrusted app.
`API_KEY_EXISTS`	Indicates that a project is using API keys instead of standard authentication.
`API_KEY_NOT_ROTATED`	Indicates that the API key hasn't been rotated for more than 90 days.

Compute image vulnerability findings

The `COMPUTE_IMAGE_SCANNER` scanner detects vulnerabilities related to Google Cloud image configurations.

Table 3. Compute image scanner

Category	Finding description
`PUBLIC_COMPUTE_IMAGE`	Indicates that a Compute Engine instance is using a public image.

Compute instance vulnerability findings

The `COMPUTE_INSTANCE_SCANNER` scanner detects vulnerabilities related to Google Cloud instance configurations.

Table 4. Compute instance scanner

Category	Finding description
`COMPUTE_PROJECT_WIDE_SSH_KEYS_ALLOWED`	Indicates that project-wide SSH keys are used, allowing login to all instances in the project.
`COMPUTE_SERIAL_PORTS_ENABLED`	Indicates that serial ports are enabled for an instance, allowing connections to the instance's serial console.
`DISK_CSEK_DISABLED`	Indicates that disks on this VM are not encrypted with Customer Supplied Encryption Keys (CSEK). This scanner requires additional configuration to enable. To enable this detector, apply the security mark (https://cloud.google.com/security-command-center/docs/how-to-security-marks) `enforce_customer_supplied_disk_encryption_keys` with a value of `true` to the assets you want to monitor.

FULL_API_ACCESS	Indicates that an instance is configured to use the default service account with full access to all Google Cloud APIs.
IP_FORWARDING_ENABLED	Indicates that IP forwarding is enabled on Instances.
OS_LOGIN_DISABLED	Indicates that OS Login is disabled on this instance.
PUBLIC_IP_ADDRESS	Indicates that an instance has a public IP address.
WEAK_SSL_POLICY	Indicates that an instance has a weak SSL policy.

Container vulnerability findings

These finding types all relate to GKE container configurations, and belong to the `CONTAINER_SCANNER` scanner type.

Table 5. Container scanner

Category	Finding description
AUTO_REPAIR_DISABLED	Indicates that the GKE clusters auto repair feature, which keeps nodes in a healthy, running state, is disabled.
AUTO_UPGRADE_DISABLED	Indicates that GKE clusters auto upgrade feature, which keeps clusters and node pools on the latest stable version of Kubernetes, is disabled.
CLUSTER_LOGGING_DISABLED	Indicates that logging is not enabled for a GKE cluster.
CLUSTER_MONITORING_DISABLED	Indicates that Stackdriver Monitoring is disabled on GKE clusters.
CLUSTER_PRIVATE_GOOGLE_ACCESS_DISABLED	Indicates that cluster hosts are not configured to use only private, internal IP addresses to access Google APIs.
COS_NOT_USED	Indicates that Compute Engine VMs are not using the Container-Optimized OS designed for running Docker containers on Google Cloud securely.
IP_ALIAS_DISABLED	Indicates that a GKE cluster was created with Alias IP ranges enabled.
LEGACY_AUTHORIZATION_ENABLED	Indicates that Legacy Authorization is enabled on GKE clusters.

`LEGACY_METADATA_ENABLED`	Indicates that legacy metadata is enabled on GKE clusters.
`MASTER_AUTHORIZED_NETWORKS_DISABLED`	Indicates that **Master authorized networks** is not enabled on GKE clusters.
`NETWORK_POLICY_DISABLED`	Indicates that Network policy is disabled on GKE clusters.
`OVER_PRIVILEGED_ACCOUNT`	Indicates that a service account has overly broad project access in a cluster.
`OVER_PRIVILEGED_SCOPES`	Indicates that a node service account has broad access scopes.
`POD_SECURITY_POLICY_DISABLED`	Indicates that **`PodSecurityPolicy`** is disabled on a GKE cluster.
`PRIVATE_CLUSTER_DISABLED`	Indicates that a GKE cluster has a Private cluster disabled.
`WEB_UI_ENABLED`	Indicates that the GKE web UI (dashboard) is enabled.
`WORKLOAD_IDENTITY_DISABLED`	Indicates that Workload Identity is disabled on a GKE cluster.

Dataset vulnerability findings

Vulnerabilities of this scanner type all relate to BigQuery Dataset configurations, and belong to the `DATASET_SCANNER` scanner type.

Table 6. Dataset scanner

Category	Finding description
`PUBLIC_DATASET`	Indicates that a dataset is configured to be open to public access.

DNS vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud DNS configurations, and belong to the `DNS_SCANNER` scanner type.

Table 7. DNS scanner

Category	Finding description

`DNSSEC_DISABLED`	Indicates that DNSSEC is disabled for Cloud DNS zones.
`RSASHA1_FOR_SIGNING`	Indicates that RSASHA1 is used for key signing in Cloud DNS zones.

Firewall vulnerability findings

Vulnerabilities of this scanner type all relate to firewall configurations, and belong to the `FIREWALL_SCANNER` scanner type.

Table 8. Firewall scanner

Category	Finding description
`OPEN_FIREWALL`	Indicates that a firewall is configured to be open to public access.
`OPEN_RDP_PORT`	Indicates that a firewall is configured to have an open RDP port that allows generic access.
`OPEN_SSH_PORT`	Indicates that a firewall is configured to have an open SSH port that allows generic access.

IAM vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud Identity and Access Management (Cloud IAM) configuration, and belong to the `IAM_SCANNER` scanner type.

Table 9. IAM Scanner

Category	Finding description
`ADMIN_SERVICE_ACCOUNT`	Indicates that there is a service account configured with administrator roles.
`KMS_ROLE_SEPARATION`	Indicates that separation of duties is not enforced, and a user exists who has any of the: Cloud Key Management Service (Cloud KMS) CryptoKey Encrypter/Decrypter, Encrypter, or Decrypter roles at the same time.
`NON_ORG_IAM_MEMBER`	Indicates that there is a user who isn't using organizational credentials.
`OVER_PRIVILEGED_SERVICE_ACCOUNT_USER`	Indicates that a user has the Service Account User role at the

	project level, instead of for a specific service account.
`SERVICE_ACCOUNT_ROLE_SEPARATION`	Indicates that a user has been assigned the Service Account Admin and Service Account User roles. This violates the "Separation of Duties" principle.

KMS vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud KMS configurations, and belong to the `KMS_SCANNER` scanner type.

Table 10. KMS scanner

Category	Finding description
`KMS_KEY_NOT_ROTATED`	Indicates that rotation isn't configured on a Cloud KMS encryption key.

Logging vulnerability findings(:#logging-findings}

Vulnerabilities of this scanner type all relate to logging configurations, and belong to the `LOGGING_SCANNER` scanner type.

Table 11. Logging scanner

Category	Finding description
`AUDIT_LOGGING_DISABLED`	Indicates that audit logging has been disabled for this resource.
`BUCKET_LOGGING_DISABLED`	Indicates that there is a storage bucket without logging enabled.
`LOG_NOT_EXPORTED`	Indicates there is a resource that does not have an appropriate log sink configured.
`OBJECT_VERSIONING_DISABLED`	Indicates that object versioning isn't enabled on a storage bucket where sinks are configured.

Monitoring vulnerability findings

Vulnerabilities of this scanner type all relate to monitoring configurations, and belong to the `MONITORING_SCANNER` type. All Monitoring scanner finding properties will include:

- The `RecommendedLogFilter` to use in creating the log metrics.
- The `QualifiedLogMetricNames` that cover the conditions listed in the recommended log filter.
- The `AlertPolicyFailureReasons` that indicate if the project does not have alert policies created for any of the qualified log metrics or the existing alert policies do not have the recommended settings.

Table 12. Monitoring scanner

Category	Finding description
`AUDIT_CONFIG_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor Audit Configuration Changes.
`BUCKET_IAM_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor Cloud Storage Cloud IAM permission changes.
`CUSTOM_ROLE_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor Custom Role changes.
`FIREWALL_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor VPC Network Firewall rule changes.
`NETWORK_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor VPC network changes.
`OWNER_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor Project Ownership assignments or changes.
`ROUTE_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor VPC network route changes.
`SQL_INSTANCE_NOT_MONITORED`	Indicates that log metrics and alerts aren't configured to monitor Cloud SQL instance configuration changes.

Network vulnerability findings

Vulnerabilities of this scanner type all relate to an organization's network configurations, and belong to the `NETWORK_SCANNER` type.

Table 13. Network scanner

Category	Finding description
DEFAULT_NETWORK	Indicates that the default network exists in a project.
LEGACY_NETWORK	Indicates that a legacy network exists in a project.

SSH password vulnerability findings

Vulnerabilities of this scanner type all relate to passwords, and belong to the `SSH_PASSWORD` type.

Table 14. SSH password scanner

Category	Finding description
WEAK_SSH_PASSWORD	Indicates that a resource has a weak SSH password.

SQL vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud SQL configurations, and belong to the `SQL_SCANNER` type.

Table 15. SQL scanner

Category	Finding description
AUTO_BACKUP_DISABLED	Indicates that a Cloud SQL database doesn't have automatic backups enabled.
PUBLIC_SQL_INSTANCE	Indicates that a Cloud SQL database instance accepts connections from all IP addresses.
SSL_NOT_ENFORCED	Indicates that a Cloud SQL database instance doesn't require all incoming connections to use SSL.
SQL_NO_ROOT_PASSWORD	Indicates that a Cloud SQL database doesn't have a password configured for the root account.
SQL_WEAK_ROOT_PASSWORD	Indicates that a Cloud SQL database has a weak password configured for the

	root account.

Storage vulnerability findings

Vulnerabilities of this scanner type all relate to Cloud Storage Buckets configurations, and belong to the`STORAGE_SCANNER`type.

Table 16. Storage scanner

Category	Finding description
`BUCKET_POLICY_ONLY_DISABLED`	Indicates that **`uniform bucket-level access`**, previously called **`Bucket Policy Only`**, isn't configured.
`LOGGING_DISABLED`	Indicates that logging is disabled for a Cloud Storage bucket.
`PUBLIC_BUCKET_ACL`	Indicates that a Cloud Storage bucket is publicly accessible.

Subnetwork vulnerability findings

Vulnerabilities of this scanner type all relate to an organization's subnetwork configurations, and belong to the`SUBNETWORK_SCANNER`type.

Table 17. Subnetwork scanner

Category	Finding description
`FLOW_LOGS_DISABLED`	Indicates there is a VPC subnetwork that has flow logs disabled.
`PRIVATE_GOOGLE_ACCESS_DISABLED`	Indicates private subnets without access to Google public APIs.

What's next

- Learn how to use Security Health Analytics (https://cloud.google.com/security-command-center/docs/how-to-manage-security-health-analytics).

- Read suggestions for remediating Security Health Analytics findings (https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics)

  .

Last updated January 7, 2020.