Support (https://cloud.google.com/support/) Guides

Google Cloud Platform Security Bulletins

The following security bulletins are related to Google Cloud.

GCP 2020-001

Published: 2020-01-21 | Last updated: 2020-01-21

Description

Microsoft has disclosed the following vulnerability:

Vulnerability	Severity	CVE
CVE-2020-0601 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601) — **This vulnerability is also known as the Windows Crypto API Spoofing Vulnerability**. It could be exploited to make malicious executables appear trusted or allow the attacker to conduct man-in-the-middle attacks and decrypt confidential information on user connections to the affected software.	NVD Base Score: 8.1 (High)	CVE-2020-0601 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601)

For more information, see the Microsoft disclosure (https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601).

Google Cloud impact

The infrastructure hosting the Google Cloud and Google products is not impacted by this vulnerability. Additional per-product details are listed below.

Product	Impact

Product	Impact
Compute Engine	CVE-2020-0601 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601) **For most customers, no further action is required.** Customers using Compute Engine virtual machines running Windows Server should ensure their instances have the latest Windows patch or use Windows Server images provided since 1/15/2020. Please see the Compute Engine security bulletin (https://cloud.google.com/compute/docs/security-bulletins#20200121) for more details.
Google Kubernetes Engine	CVE-2020-0601 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601) **For most customers, no further action is required.** Customers using GKE with Windows Server nodes, both the nodes and the containerized workloads that run on those nodes must be updated to patched versions to mitigate this vulnerability. Please see the GKE security bulletin (https://cloud.google.com/kubernetes-engine/docs/security-bulletins#january_21_2020) for instructions and more details.
Managed Service for Microsoft Active Directory	CVE-2020-0601 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0601) **For most customers, no further action is required.** All Managed Microsoft AD domains have been automatically updated with the patched image. Any customers manually running Microsoft Active Directory (and not utilizing Managed Microsoft AD) should ensure their instances have the latest Windows patch or use Windows Server images provided since 1/15/2020.
G Suite	**No customer action is required.** This service is not impacted by this vulnerability.
App Engine standard environment	**No customer action is required.** This service is not impacted by this vulnerability.
App Engine flexible environment	**No customer action is required.** This service is not impacted by this vulnerability.

Product	Impact
Cloud Run	**No customer action is required.** This service is not impacted by this vulnerability.
Cloud Functions	**No customer action is required.** This service is not impacted by this vulnerability.
Cloud Composer	**No customer action is required.** This service is not impacted by this vulnerability.
Dataflow	**No customer action is required.** This service is not impacted by this vulnerability.
Dataproc	**No customer action is required.** This service is not impacted by this vulnerability.
Cloud SQL	**No customer action is required.** This service is not impacted by this vulnerability.

GCP 2019-001

Published: 2019-11-12 | Last updated: 2019-11-12

Description

Intel has disclosed the following vulnerabilities:

Vulnerability	SeverityCVE

Vulnerability	Severity	CVE
CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) — **This vulnerability referred to as TSX Async Abort (TAA) can be used to exploit speculative execution within a TSX transaction.** This vulnerability potentially allows data to be exposed via the same microarchitectural data structures exposed by Microarchitectural Data Sampling (MDS) (https://support.google.com/faqs/answer/9330250).	Medium	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135)
CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) — **This is a Denial of Service (DoS) vulnerability affecting virtual machine hosts (not guests).** This issue is known as "Machine Check Error on Page Size Change."	Medium	CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207)

For more information, see the Intel disclosures:

- Intel Blog Post (https://blogs.intel.com/technology/2019/11/ipas-november-2019-intel-platform-update-ipu/)
- Intel's Developer Guidance Site (https://software.intel.com/security-software-guidance/software-guidance/):
  - Machine Check Error on Page Size Change (https://software.intel.com/security-software-guidance/insights/deep-dive-machine-check-error-avoidance-page-size-change)
  - TSX Asynchronous Abort (https://software.intel.com/security-software-guidance/insights/deep-dive-intel-transactional-synchronization-extensions-intel-tsx-asynchronous-abort)

Google Cloud impact

The infrastructure hosting the Google Cloud and Google products is protected from these vulnerabilities. Additional per-product details are listed below.

Product	Impact

Product	Impact
Compute Engine	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) **For most customers, no additional action is required.** N2, C2 or M2 customers running untrusted code in their own multi-tenant services within Compute Engine virtual machines should stop and start their VMs (https://cloud.google.com/compute/docs/instances/stop-start-instance) to ensure that they have the latest security mitigations. ★ **Note**: For more details, see the Compute Engine security bulletin (https://cloud.google.com/compute/docs/security-bulletins). CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) **For all customers, no additional action is required.**
Google Kubernetes Engine	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) **For most customers, no additional action is required.** If you use node pools with N2, M2, or C2 nodes, and those nodes run untrusted code inside your own multi-tenant GKE clusters, then you should restart your nodes. If you want to restart all nodes in your node pool, upgrade the affected node pool (https://cloud.google.com/kubernetes-engine/docs/how-to/upgrading-a-cluster#upgrade_nodes) . ★ **Note**: You can specify the same GKE version for an upgrade to your node pool. For more details, see the GKE security bulletin (https://cloud.google.com/kubernetes-engine/docs/security-bulletins#november_12_2019). CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) **For all customers, no additional action is required.**
App Engine standard environment	**No additional action is required.**

Product	Impact
App Engine flexible environment	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) **No additional action is required.** Customers should review Intel best practices with respect to application-level sharing which may occur between hyperthreads within a Flex VM. CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) **No additional action is required.**
Cloud Run	**No additional action is required.**
Cloud Functions	**No additional action is required.**
Cloud Composer	**No additional action is required.**
Dataflow	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) **For most customers, no additional action is required.** Dataflow customers who run multiple untrusted workloads on N2, C2, or M2 Compute Engine VMs managed by Dataflow and are concerned about intra-guest attacks should consider restarting (https://cloud.google.com/dataflow/pipelines/stopping-a-pipeline) any streaming pipelines that are currently running. Optionally, batch pipelines can be cancelled and re-run. No action is required for pipelines launched after today. CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) **For all customers, no additional action is required.**

Product	Impact
Dataproc	CVE-2019-11135 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2019-11135) **For most customers, no additional action is required.** Cloud Dataproc customers who run multiple, untrusted workloads on the same Cloud Dataproc cluster running on Compute Engine N2, C2 or M2 VMs and are concerned about intra-guest attacks, should redeploy their clusters (https://cloud.google.com/dataproc/docs/guides/create-cluster). CVE-2018-12207 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=2018-12207) **For all customers, no additional action is required.**
Cloud SQL	**No additional action is required.**

Last updated January 21, 2020.