How to read the report | **Suppressing false positives** | **Getting Help: github issues**

Project:

Scan Information (show all):

- *dependency-check version*: 6.0.5
- *Report Generated On*: Tue, 12 Jan 2021 14:03:01 -0800
- *Dependencies Scanned*: 212 (212 unique)
- *Vulnerable Dependencies*: 15
- *Vulnerabilities Found*: 185
- *Vulnerabilities Suppressed*: 0
- ...

Summary

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
github.com/apache/thrift:0.12.0	cpe:2.3:a:apache:thrift:0.12.0:*:*:*:*:*:*:*	pkg:golang/github.com/apache/thrift@0.12.0	HIGH	2	Highest	6
github.com/docker/distribution:2.7.1+incompatible	cpe:2.3:a:docker:docker:2.7.1:*:*:*:*:*:*:*	pkg:golang/github.com/docker/distribution@2.7.1%2Bincompatible	HIGH	6	Low	6
github.com/docker/docker:1.4.2-0.20200213202729-31a86c4ab209	cpe:2.3:a:docker:docker:1.4.2.0.20200213202729.31.a86.c4:ab209:*:*:*:*:*:*	pkg:golang/github.com/docker/docker@1.4.2-0.20200213202729-31a86c4ab209	CRITICAL	14	Highest	6
github.com/docker/go-connections:0.4.0	cpe:2.3:a:connections_project:connections:0.4.0:*:*:*:*:*:*:*	pkg:golang/github.com/docker/go-connections@0.4.0	HIGH	1	Highest	6
github.com/docker/go-units:0.4.0	cpe:2.3:a:docker:docker:0.4.0:*:*:*:*:*:*:*	pkg:golang/github.com/docker/go-units@0.4.0	CRITICAL	21	Low	6
github.com/go-sql-driver/mysql:1.5.0	cpe:2.3:a:mysql:mysql:1.5.0:*:*:*:*:*:*:*	pkg:golang/github.com/go-sql-driver/mysql@1.5.0	HIGH	13	High	6
github.com/grpc-ecosystem/go-grpc-middleware:1.2.0	cpe:2.3:a:grpc:grpc:1.2.0:*:*:*:*:*:*:*	pkg:golang/github.com/grpc-ecosystem/go-grpc-middleware@1.2.0	CRITICAL	3	Highest	6
github.com/grpc-ecosystem/grpc-gateway:1.14.3	cpe:2.3:a:grpc:grpc:1.14.3:*:*:*:*:*:*:*	pkg:golang/github.com/grpc-ecosystem/grpc-gateway@1.14.3	HIGH	1	Highest	6
github.com/prometheus/client_golang:0.9.3-0.20190127221311-3c4408c8b829	cpe:2.3:a:prometheus:prometheus:0.9.3.0:*:*:*:*:*:*:*	pkg:golang/github.com/prometheus/client_golang@0.9.3-0.20190127221311-3c4408c8b829	MEDIUM	1	Low	6
github.com/prometheus/client_model:0.0.0-20190812154241-14fe0d1b01d4	cpe:2.3:a:prometheus:prometheus:0.0.0:*:*:*:*:*:*:*	pkg:golang/github.com/prometheus/client_model@0.0.0-20190812154241-14fe0d1b01d4	MEDIUM	1	Low	6
github.com/prometheus/common:0.2.0	cpe:2.3:a:prometheus:prometheus:0.2.0:*:*:*:*:*:*:*	pkg:golang/github.com/prometheus/common@0.2.0	MEDIUM	1	Low	6
github.com/prometheus/procfs:0.0.0-20190117184657-bf6a532e95b1	cpe:2.3:a:prometheus:prometheus:0.0.0:*:*:*:*:*:*:*	pkg:golang/github.com/prometheus/procfs@0.0.0-20190117184657-bf6a532e95b1	MEDIUM	1	Low	6
github.com/robfig/cron/v3:3.0.1	cpe:2.3:a:cron_project:cron:3.0.1:*:*:*:*:*:*:*	pkg:golang/github.com/robfig/cron/v3@3.0.1	MEDIUM	3	Low	6
github.com/xanzy/go-gitlab:0.15.0	cpe:2.3:a:gitlab:gitlab:0.15.0:*:*:*:*:*:*:*	pkg:golang/github.com/xanzy/go-gitlab@0.15.0	CRITICAL	113	High	6
modernc.org/file:1.0.0	cpe:2.3:a:file_project:file:1.0.0:*:*:*:*:*:*:*	pkg:golang/modernc.org/file@1.0.0	CRITICAL	4	High	3

Dependencies

github.com/apache/thrift:0.12.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/apache/thrift/0.12.0

Evidence

Identifiers

- pkg:golang/github.com/apache/thrift@0.12.0 (*Confidence*:Highest)
- cpe:2.3:a:apache:thrift:0.12.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2019-0205 suppress

In Apache Thrift all versions up to and including 0.12.0, a server or client may run into an endless loop when feed with specific input data. Because the issue had already been partially fixed in version 0.11.0, depending on the installed version it affects only certain language bindings.

CWE-835 Loop with Unreachable Exit Condition ('Infinite Loop')

CVSSv2:

- Base Score: HIGH (7.8)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:C

CVSSv3:

- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:

- MISC - http://mail-archives.apache.org/mod_mbox/thrift-dev/201910.mbox/%3CVI1PR0101MB2142E0EA19F582429C3AEBCBB1920%40VI1PR0101MB2142.eurprd01.prod.exchangelabs.com%3E
- MLIST - [cassandra-commits] 20191113 [jira] [Created] (CASSANDRA-15415) CVE-2019-0205 (Apache Thrift all versions up to and including 0.12.0 vulnerable) of severity 7.5
- MLIST - [cassandra-commits] 20191113 [jira] [Created] (CASSANDRA-15420) CVE-2019-0205(Apache Thrift all versions up to and including 0.12.0) on version Cassendra 3.11.4
- MLIST - [cassandra-commits] 20200604 [jira] [Created] (CASSANDRA-15856) Security vulnerabilities with dependency jars of Cassandra 3.11.6
- MLIST - [hive-dev] 20200116 [jira] [Created] (HIVE-22738) CVE-2019-0205
- MLIST - [hive-issues] 20200116 [jira] [Updated] (HIVE-22738) CVE-2019-0205
- MLIST - [thrift-commits] 20200208 [thrift] 01/01: THRIFT-5075: Backport changes for CVE-2019-0205 to 0.9.3.1 branch
- MLIST - [thrift-dev] 20191106 [jira] [Assigned] (THRIFT-4997) Nexus Scan Reporting Security issue CVE-2019-0205 for Thrift:
- MLIST - [thrift-dev] 20191106 [jira] [Comment Edited] (THRIFT-4997) Nexus Scan Reporting Security issue CVE-2019-0205 for Thrift:
- MLIST - [thrift-dev] 20191106 [jira] [Created] (THRIFT-4997) Nexus Scan Reporting Security issue CVE-2019-0205 for Thrift:
- MLIST - [thrift-dev] 20191106 [jira] [Resolved] (THRIFT-4997) Nexus Scan Reporting Security issue CVE-2019-0205 for Thrift:
- MLIST - [thrift-dev] 20191106 [jira] [Updated] (THRIFT-4997) Nexus Scan Reporting Security issue CVE-2019-0205 for Thrift:
- MLIST - [thrift-dev] 20200124 [jira] [Commented] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200124 [jira] [Created] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200125 [jira] [Comment Edited] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200125 [jira] [Commented] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200127 [jira] [Commented] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200208 [jira] [Comment Edited] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version
- MLIST - [thrift-dev] 20200208 [jira] [Commented] (THRIFT-5075) Backport fixes for CVE-2019-0205 to (Java) 0.9.3-1 version

- MLIST - [thrift-notifications] 20200813 [GitHub] [thrift] kevinsookocheff-wf commented on pull request #1993: THRIFT-5075: Backport changes for CVE-2019-0205 to 0.9.3.1 branch
- MLIST - [thrift-user] 20191107 CVE-2019-0205
- MLIST - [thrift-user] 20191108 Re: CVE-2019-0205
- REDHAT - RHSA-2020:0804
- REDHAT - RHSA-2020:0805
- REDHAT - RHSA-2020:0806
- REDHAT - RHSA-2020:0811

Vulnerable Software & Versions:

- cpe:2.3:a:apache:thrift:*:*:*:*:*:*:*:* versions up to (including) 0.12.0

CVE-2019-0210 suppress

In Apache Thrift 0.9.3 to 0.12.0, a server implemented in Go using TJSONProtocol or TSimpleJSONProtocol may panic when feed with invalid input data.

CWE-125 Out-of-bounds Read

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - http://mail-archives.apache.org/mod_mbox/thrift-dev/201910.mbox/%3C277A46CA87494176B1BBCF5D72624A2A%40HAGGIS%3E
- REDHAT - RHSA-2020:0804
- REDHAT - RHSA-2020:0805
- REDHAT - RHSA-2020:0806
- REDHAT - RHSA-2020:0811

Vulnerable Software & Versions:

- cpe:2.3:a:apache:thrift:*:*:*:*:*:*:*:* versions from (including) 0.9.3; versions up to (including) 0.12.0

github.com/docker/distribution:2.7.1+incompatible

File Path: /Users/akhode/v4/dss/go.mod:github.com/docker/distribution/2.7.1+incompatible

Evidence

Identifiers

- pkg:golang/github.com/docker/distribution@2.7.1%2Bincompatible (*Confidence*:Highest)
- cpe:2.3:a:docker:docker:2.7.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2018-10892 suppress

The default OCI linux spec in oci/defaults{_linux}.go in Docker/Moby from 1.11 to current does not block /proc/acpi pathnames. The flaw allows an attacker to modify host's hardware like enabling/disabling bluetooth or turning up/down keyboard brightness.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10892
- CONFIRM - https://github.com/moby/moby/pull/37404
- REDHAT - RHBA-2018:2796
- REDHAT - RHSA-2018:2482
- REDHAT - RHSA-2018:2729
- SUSE - openSUSE-SU-2019:2021

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:enterprise_edition:*:*:* versions from (including) 1.11; versions up to (including) 18.03.1
- ...

CVE-2019-13139 suppress

In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the "docker build" command would be able to gain command execution. An issue exists in the way "docker build" processes remote git URLs, and results in command injection into the underlying "git clone" command, leading to code execution in the context of the user executing the "docker build" command. This occurs because git ref can be misinterpreted as a flag.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.4)
- Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190910-0001/
- DEBIAN - DSA-4521
- MISC - https://docs.docker.com/engine/release-notes/#18094
- MISC - https://github.com/moby/moby/pull/38944
- MISC - https://staaldraad.github.io/post/2019-07-16-cve-2019-13139-docker-build/
- REDHAT - RHBA-2019:3092

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:enterprise:*:*:* versions up to (excluding) 18.09.4

CVE-2019-13509 suppress

In Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploy is run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if they resend the secret.

CWE-532 Information Exposure Through Log Files

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- BID - 109253
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190828-0003/
- DEBIAN - DSA-4521
- FEDORA - FEDORA-2019-4bed83e978
- FEDORA - FEDORA-2019-5b54793a4a
- MISC - https://docs.docker.com/engine/release-notes/
- SUSE - openSUSE-SU-2019:2021

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (excluding) 18.09.8
- ...

CVE-2019-16884 suppress

runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- FEDORA - FEDORA-2019-3fc86a518b
- FEDORA - FEDORA-2019-96946c39dd
- FEDORA - FEDORA-2019-bd4843561c
- GENTOO - GLSA-202003-21
- MISC - https://github.com/opencontainers/runc/issues/2128
- REDHAT - RHSA-2019:3940
- REDHAT - RHSA-2019:4074
- REDHAT - RHSA-2019:4269
- SUSE - openSUSE-SU-2019:2418
- SUSE - openSUSE-SU-2019:2434
- SUSE - openSUSE-SU-2020:0045
- UBUNTU - USN-4297-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (including) 19.03.2
- ...

CVE-2019-5736 suppress

runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (8.6)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
- BID - 106976
- CISCO - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc
- CONFIRM - https://security.netapp.com/advisory/ntap-20190307-0008/
- CONFIRM - https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03410944
- CONFIRM - https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03913en_us
- CONFIRM - https://support.mesosphere.com/s/article/Known-Issue-Container-Runtime-Vulnerability-MSPH-2019-0003
- CONFIRM - https://www.synology.com/security/advisory/Synology_SA_19_06
- EXPLOIT-DB - 46359
- EXPLOIT-DB - 46369
- FEDORA - FEDORA-2019-2baa1f7b19
- FEDORA - FEDORA-2019-6174b47003
- FEDORA - FEDORA-2019-bc70b381ad
- FEDORA - FEDORA-2019-c1dac1b3b8
- GENTOO - GLSA-202003-21
- MISC - https://access.redhat.com/security/cve/cve-2019-5736
- MISC - https://access.redhat.com/security/vulnerabilities/runcescape
- MISC - https://aws.amazon.com/security/security-bulletins/AWS-2019-002/
- MISC - https://azure.microsoft.com/en-us/updates/cve-2019-5736-and-runc-vulnerability/
- MISC - https://azure.microsoft.com/en-us/updates/iot-edge-fix-cve-2019-5736/
- MISC - https://blog.dragonsector.pl/2019/02/cve-2019-5736-escape-from-docker-and.html
- MISC - https://brauner.github.io/2019/02/12/privileged-containers.html
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=1121967
- MISC - https://cloud.google.com/kubernetes-engine/docs/security-bulletins#february-11-2019-runc
- MISC - https://github.com/Frichetten/CVE-2019-5736-PoC
- MISC - https://github.com/docker/docker-ce/releases/tag/v18.09.2
- MISC - https://github.com/opencontainers/runc/commit/0a8e4117e7f715d5fbeef398405813ce8e88558b
- MISC - https://github.com/opencontainers/runc/commit/6635b4f0c6af3810594d2770f662f34ddc15b40d
- MISC - https://github.com/q3k/cve-2019-5736-poc
- MISC - https://github.com/rancher/runc-cve
- MISC - https://kubernetes.io/blog/2019/02/11/runc-and-cve-2019-5736/
- MISC - https://www.openwall.com/lists/oss-security/2019/02/11/2
- MISC - https://www.twistlock.com/2019/02/11/how-to-mitigate-cve-2019-5736-in-runc-and-docker/
- MLIST - [dlab-dev] 20190524 [jira] [Created] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190524 [jira] [Updated] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190923 [jira] [Assigned] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20200525 [jira] [Deleted] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- MLIST - [mesos-dev] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [mesos-user] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190628 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20191023 Membership application for linux-distros - VMware
- MLIST - [oss-security] 20191029 Re: Membership application for linux-distros - VMware
- REDHAT - RHSA-2019:0303
- REDHAT - RHSA-2019:0304
- REDHAT - RHSA-2019:0401
- REDHAT - RHSA-2019:0408
- REDHAT - RHSA-2019:0975
- SUSE - openSUSE-SU-2019:1079
- SUSE - openSUSE-SU-2019:1227
- SUSE - openSUSE-SU-2019:1275
- SUSE - openSUSE-SU-2019:1444
- SUSE - openSUSE-SU-2019:1481
- SUSE - openSUSE-SU-2019:1499
- SUSE - openSUSE-SU-2019:1506
- SUSE - openSUSE-SU-2019:2021
- SUSE - openSUSE-SU-2019:2245
- SUSE - openSUSE-SU-2019:2286
- UBUNTU - USN-4048-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 18.09.2
- ...

CVE-2020-27534 suppress

util/binfmt_misc/check.go in Builder in Docker Engine before 19.03.9 calls os.OpenFile with a potentially unsafe qemu-check temporary pathname, constructed with an empty first argument in an ioutil.TempDir call.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - http://web.archive.org/web/20200530054359/https://docs.docker.com/engine/release-notes/
- MISC - https://github.com/moby/buildkit/pull/1462
- MISC - https://github.com/moby/moby/pull/40877
- MISC - https://golang.org/pkg/io/ioutil/#TempDir
- MISC - https://golang.org/pkg/os/#TempDir

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 19.03.9

github.com/docker/docker:1.4.2-0.20200213202729-31a86c4ab209

File Path: /Users/akhode/v4/dss/go.mod:github.com/docker/docker/1.4.2-0.20200213202729-31a86c4ab209

Evidence

Identifiers

- pkg:golang/github.com/docker/docker@1.4.2-0.20200213202729-31a86c4ab209 (*Confidence*:Highest)
- cpe:2.3:a:docker:docker:1.4.2.0.20200213202729.31.a86.c4:ab209:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2014-0048 suppress

An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/18
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/22
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/23
- MISC - https://access.redhat.com/security/cve/cve-2014-0048
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-0048
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=CVE-2014-0048
- MISC - https://security-tracker.debian.org/tracker/CVE-2014-0048
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.5.0

CVE-2014-8178 suppress

Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 do not use a globally unique identifier to store image layers, which makes it easier for attackers to poison the image cache via a crafted image in pull or push commands.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: LOW (1.9)
- Vector: /AV:L/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://www.docker.com/legal/docker-cve-database
- MISC - http://lists.opensuse.org/opensuse-security-announce/2015-10/msg00014.html
- MISC - http://lists.opensuse.org/opensuse-updates/2015-10/msg00036.html
- MISC - https://github.com/docker/docker/blob/master/CHANGELOG.md#183-2015-10-12
- MISC - https://groups.google.com/forum/#!msg/docker-dev/bWVVtLNbFy8/UaefOgMOCAAJ

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.8.3
- ...

CVE-2014-8179 suppress

Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 does not properly validate and extract the manifest object from its JSON representation during a pull, which allows attackers to inject new attributes in a JSON object and bypass pull-by-digest validation.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://www.docker.com/legal/docker-cve-database
- MISC - http://lists.opensuse.org/opensuse-security-announce/2015-10/msg00014.html
- MISC - http://lists.opensuse.org/opensuse-updates/2015-10/msg00036.html
- MISC - https://blog.docker.com/2015/10/security-release-docker-1-8-3-1-6-2-cs7/
- MISC - https://github.com/docker/docker/blob/master/CHANGELOG.md#183-2015-10-12
- MISC - https://groups.google.com/forum/#!msg/docker-dev/bWVVtLNbFy8/UaefOgMOCAAJ

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.8.3
- ...

CVE-2015-3627 suppress

Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

References:
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6
- ...

CVE-2015-3630 suppress

Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

References:
- BID - 74566
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6

CVE-2015-3631 suppress

Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an image that allows volumes to override files in /proc.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:L/AC:L/Au:N/C:N/I:P/A:P

References:
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6

CVE-2016-3697 suppress

libcontainer/user/user.go in runC before 0.1.0, as used in Docker before 1.11.2, improperly treats a numeric UID as a potential username, which allows local users to gain privileges via a numeric username in the password file in a container.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://github.com/docker/docker/issues/21436
- CONFIRM - https://github.com/opencontainers/runc/commit/69af385de62ea68e2e608335cffbb0f4aa3db091
- CONFIRM - https://github.com/opencontainers/runc/pull/708
- CONFIRM - https://github.com/opencontainers/runc/releases/tag/v0.1.0
- GENTOO - GLSA-201612-28
- REDHAT - RHSA-2016:1034
- REDHAT - RHSA-2016:2634
- SUSE - openSUSE-SU-2016:1417

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.11.1
- ...

CVE-2017-14992 suppress

Lack of content verification in Docker-CE (Also known as Moby) versions 1.12.6-0, 1.10.3, 17.03.0, 17.03.1, 17.03.2, 17.06.0, 17.06.1, 17.06.2, 17.09.0, and earlier allows a remote attacker to cause a Denial of Service via a crafted image layer payload, aka gzip bombing.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://github.com/moby/moby/issues/35075
- MISC - https://blog.cloudpassage.com/2017/10/13/discovering-docker-cve-2017-14992/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (including) 1.10.3
- ...

CVE-2019-13139 suppress

In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the "docker build" command would be able to gain command execution. An issue exists in the way "docker build" processes remote git URLs, and results in command injection into the underlying "git clone" command, leading to code execution in the context of the user executing the "docker build" command. This occurs because git ref can be misinterpreted as a flag.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.4)
- Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190910-0001/
- DEBIAN - DSA-4521

- MISC - https://docs.docker.com/engine/release-notes/#18094
- MISC - https://github.com/moby/moby/pull/38944
- MISC - https://staaldraad.github.io/post/2019-07-16-cve-2019-13139-docker-build/
- REDHAT - RHBA-2019:3092

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:enterprise:*:*:* versions up to (excluding) 18.09.4

CVE-2019-13509 suppress

In Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploy is run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if they resend the secret.

CWE-532 Information Exposure Through Log Files

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- BID - 109253
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190828-0003/
- DEBIAN - DSA-4521
- FEDORA - FEDORA-2019-4bed83e978
- FEDORA - FEDORA-2019-5b54793a4a
- MISC - https://docs.docker.com/engine/release-notes/
- SUSE - openSUSE-SU-2019:2021

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (excluding) 18.09.8
- ...

CVE-2019-15752 suppress

Docker Desktop Community Edition before 2.1.0.1 allows local users to gain privileges by placing a Trojan horse docker-credential-wincred.exe file in %PROGRAMDATA%\DockerDesktop\version-bin\ as a low-privilege user, and then waiting for an admin or service user to authenticate with Docker, restart Docker, or run 'docker login' to force the command.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

References:
- MISC - http://packetstormsecurity.com/files/157404/Docker-Credential-Wincred.exe-Privilege-Escalation.html
- MISC - https://medium.com/@morgan.henry.roman/elevation-of-privilege-in-docker-for-windows-2fd8450b478e
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (excluding) 2.1.0.1

CVE-2019-16884 suppress

runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- FEDORA - FEDORA-2019-3fc86a518b
- FEDORA - FEDORA-2019-96946c39dd
- FEDORA - FEDORA-2019-bd4843561c
- GENTOO - GLSA-202003-21
- MISC - https://github.com/opencontainers/runc/issues/2128
- REDHAT - RHSA-2019:3940
- REDHAT - RHSA-2019:4074
- REDHAT - RHSA-2019:4269
- SUSE - openSUSE-SU-2019:2418
- SUSE - openSUSE-SU-2019:2434
- SUSE - openSUSE-SU-2020:0045
- UBUNTU - USN-4297-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (including) 19.03.2
- ...

CVE-2019-5736 suppress

runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (8.6)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
- BID - 106976
- CISCO - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc
- CONFIRM - https://security.netapp.com/advisory/ntap-20190307-0008/
- CONFIRM - https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03410944
- CONFIRM - https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03913en_us
- CONFIRM - https://support.mesosphere.com/s/article/Known-Issue-Container-Runtime-Vulnerability-MSPH-2019-0003
- CONFIRM - https://www.synology.com/security/advisory/Synology_SA_19_06
- EXPLOIT-DB - 46359
- EXPLOIT-DB - 46369
- FEDORA - FEDORA-2019-2baa1f7b19
- FEDORA - FEDORA-2019-6174b47003
- FEDORA - FEDORA-2019-bc70b381ad
- FEDORA - FEDORA-2019-c1dac1b3b8
- GENTOO - GLSA-202003-21
- MISC - https://access.redhat.com/security/cve/cve-2019-5736
- MISC - https://access.redhat.com/security/vulnerabilities/runcescape
- MISC - https://aws.amazon.com/security/security-bulletins/AWS-2019-002/
- MISC - https://azure.microsoft.com/en-us/updates/cve-2019-5736-and-runc-vulnerability/
- MISC - https://azure.microsoft.com/en-us/updates/iot-edge-fix-cve-2019-5736/
- MISC - https://blog.dragonsector.pl/2019/02/cve-2019-5736-escape-from-docker-and.html

- MISC - https://brauner.github.io/2019/02/12/privileged-containers.html
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=1121967
- MISC - https://cloud.google.com/kubernetes-engine/docs/security-bulletins#february-11-2019-runc
- MISC - https://github.com/Frichetten/CVE-2019-5736-PoC
- MISC - https://github.com/docker/docker-ce/releases/tag/v18.09.2
- MISC - https://github.com/opencontainers/runc/commit/0a8e4117e7f715d5fbeef398405813ce8e88558b
- MISC - https://github.com/opencontainers/runc/commit/6635b4f0c6af3810594d2770f662f34ddc15b40d
- MISC - https://github.com/q3k/cve-2019-5736-poc
- MISC - https://github.com/rancher/runc-cve
- MISC - https://kubernetes.io/blog/2019/02/11/runc-and-cve-2019-5736/
- MISC - https://www.openwall.com/lists/oss-security/2019/02/11/2
- MISC - https://www.twistlock.com/2019/02/11/how-to-mitigate-cve-2019-5736-in-runc-and-docker/
- MLIST - [dlab-dev] 20190524 [jira] [Created] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190524 [jira] [Updated] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190923 [jira] [Assigned] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20200525 [jira] [Deleted] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- MLIST - [mesos-dev] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [mesos-user] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190628 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20191023 Membership application for linux-distros - VMware
- MLIST - [oss-security] 20191029 Re: Membership application for linux-distros - VMware
- REDHAT - RHSA-2019:0303
- REDHAT - RHSA-2019:0304
- REDHAT - RHSA-2019:0401
- REDHAT - RHSA-2019:0408
- REDHAT - RHSA-2019:0975
- SUSE - openSUSE-SU-2019:1079
- SUSE - openSUSE-SU-2019:1227
- SUSE - openSUSE-SU-2019:1275
- SUSE - openSUSE-SU-2019:1444
- SUSE - openSUSE-SU-2019:1481
- SUSE - openSUSE-SU-2019:1499
- SUSE - openSUSE-SU-2019:1506
- SUSE - openSUSE-SU-2019:2021
- SUSE - openSUSE-SU-2019:2245
- SUSE - openSUSE-SU-2019:2286
- UBUNTU - USN-4048-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 18.09.2
- ...

CVE-2020-27534 suppress

util/binfmt_misc/check.go in Builder in Docker Engine before 19.03.9 calls os.OpenFile with a potentially unsafe qemu-check temporary pathname, constructed with an empty first argument in an ioutil.TempDir call.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - http://web.archive.org/web/20200530054359/https://docs.docker.com/engine/release-notes/
- MISC - https://github.com/moby/buildkit/pull/1462
- MISC - https://github.com/moby/moby/pull/40877
- MISC - https://golang.org/pkg/io/ioutil/#TempDir
- MISC - https://golang.org/pkg/os/#TempDir

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 19.03.9

github.com/docker/go-connections:0.4.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/docker/go-connections/0.4.0

Evidence

Identifiers

- pkg:golang/github.com/docker/go-connections@0.4.0 (*Confidence*:Highest)
- cpe:2.3:a:connections_project:connections:0.4.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2011-5254 suppress

Unspecified vulnerability in the Connections plugin before 0.7.1.6 for WordPress has unknown impact and attack vectors.

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (10.0)
- Vector: /AV:N/AC:L/Au:N/C:C/I:C/A:C

References:
- BID - 51204
- CONFIRM - http://wordpress.org/extend/plugins/connections/changelog/
- OSVDB - 78063
- SECUNIA - 47390

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:connections_project:connections:*:*:*:*:*:*:*:* versions up to (including) 0.7.1.5
- ...

github.com/docker/go-units:0.4.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/docker/go-units/0.4.0

Evidence

Identifiers

- pkg:golang/github.com/docker/go-units@0.4.0 (*Confidence*:Highest)
- cpe:2.3:a:docker:docker:0.4.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2014-0047 suppress

Docker before 1.5 allows local users to have unspecified impact via vectors involving unsafe /tmp usage.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- BID - 73315
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1063549
- MLIST - [oss-security] 20150324 Re: 2 moderate (borderline low) docker flaws fixed in >=1.5 and possibly earlier

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.4.1

CVE-2014-0048 suppress

An issue was found in Docker before 1.6.0. Some programs and scripts in Docker are downloaded via HTTP and then executed or used in unsafe ways.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/18
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/22
- MISC - http://www.openwall.com/lists/oss-security/2015/03/24/23
- MISC - https://access.redhat.com/security/cve/cve-2014-0048
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-0048
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=CVE-2014-0048
- MISC - https://security-tracker.debian.org/tracker/CVE-2014-0048
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.5.0

CVE-2014-5277 suppress

Docker before 1.3.1 and docker-py before 0.5.3 fall back to HTTP when the HTTPS connection to the registry fails, which allows man-in-the-middle attackers to conduct downgrade attacks and obtain authentication and image data by leveraging a network position between the client and the registry to block HTTPS traffic.

CWE-17

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

References:
- CONFIRM - https://groups.google.com/forum/#!topic/docker-user/oYm0i3xShJU
- SUSE - openSUSE-SU-2014:1411

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.3.0
- ...

CVE-2014-5278 suppress

A vulnerability exists in Docker before 1.2 via container names, which may collide with and override container IDs.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- MISC - https://github.com/xxg1413/docker-security/tree/master/CVE-2014-5278
- MISC - https://groups.google.com/forum/#!topic/docker-announce/IK6fQY6Jy84
- MISC - https://groups.google.com/forum/message/raw?msg=docker-user/jyf9_mYcMI8/ElZfwe2QNzYJ

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.2.0

CVE-2014-5282 suppress

Docker before 1.3 does not properly validate image IDs, which allows remote attackers to redirect to another image through the loading of untrusted images via 'docker load'.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=1168436
- CONFIRM - https://groups.google.com/forum/#!msg/docker-announce/aQoVmQlcE0A/smPuBNYf8VwJ

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.3

CVE-2014-6407 suppress

Docker before 1.3.2 allows remote attackers to write to arbitrary files and execute arbitrary code via a (1) symlink or (2) hard link attack in an image archive in a (a) pull or (b) load operation.

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:

- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:
- CONFIRM - https://docs.docker.com/v1.3/release-notes/
- FEDORA - FEDORA-2014-15779
- MLIST - [oss-security] 20141124 Docker 1.3.2 - Security Advisory [24 Nov 2014]
- SECUNIA - 60171
- SECUNIA - 60241
- SUSE - openSUSE-SU-2014:1596

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.3.1
- ...

CVE-2014-8178 suppress

Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 do not use a globally unique identifier to store image layers, which makes it easier for attackers to poison the image cache via a crafted image in pull or push commands.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: LOW (1.9)
- Vector: /AV:L/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://www.docker.com/legal/docker-cve-database
- MISC - http://lists.opensuse.org/opensuse-security-announce/2015-10/msg00014.html
- MISC - http://lists.opensuse.org/opensuse-updates/2015-10/msg00036.html
- MISC - https://github.com/docker/docker/blob/master/CHANGELOG.md#183-2015-10-12
- MISC - https://groups.google.com/forum/#!msg/docker-dev/bWVVtLNbFy8/UaefOgMOCAAJ

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.8.3
- ...

CVE-2014-8179 suppress

Docker Engine before 1.8.3 and CS Docker Engine before 1.6.2-CS7 does not properly validate and extract the manifest object from its JSON representation during a pull, which allows attackers to inject new attributes in a JSON object and bypass pull-by-digest validation.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://www.docker.com/legal/docker-cve-database
- MISC - http://lists.opensuse.org/opensuse-security-announce/2015-10/msg00014.html
- MISC - http://lists.opensuse.org/opensuse-updates/2015-10/msg00036.html
- MISC - https://blog.docker.com/2015/10/security-release-docker-1-8-3-1-6-2-cs7/
- MISC - https://github.com/docker/docker/blob/master/CHANGELOG.md#183-2015-10-12
- MISC - https://groups.google.com/forum/#!msg/docker-dev/bWVVtLNbFy8/UaefOgMOCAAJ

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.8.3
- ...

CVE-2014-9356 suppress

Path traversal vulnerability in Docker before 1.3.3 allows remote attackers to write to arbitrary files and bypass a container protection mechanism via a full pathname in a symlink in an (1) image or (2) build in a Dockerfile.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: HIGH (8.5)
- Vector: /AV:N/AC:L/Au:N/C:N/I:C/A:P

CVSSv3:
- Base Score: HIGH (8.6)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N

References:
- BUGTRAQ - 20141212 Docker 1.3.3 - Security Advisory [11 Dec 2014]
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=1172761

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 1.3.3

CVE-2014-9358 suppress

Docker before 1.3.3 does not properly validate image IDs, which allows remote attackers to conduct path traversal attacks and spoof repositories via a crafted image in a (1) "docker load" operation or (2) "registry communications."

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (6.4)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

References:
- BUGTRAQ - 20141212 Docker 1.3.3 - Security Advisory [11 Dec 2014]
- CONFIRM - https://groups.google.com/forum/#!msg/docker-user/nFAz-B-n4Bw/0wr3wvLsnUwJ

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.3.2

CVE-2015-3627 suppress

Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

References:
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6
- ...

CVE-2015-3630 suppress

Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade

attacks via a crafted image.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

References:
- BID - 74566
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6

CVE-2015-3631 suppress

Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an image that allows volumes to override files in /proc.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:L/AC:L/Au:N/C:N/I:P/A:P

References:
- CONFIRM - https://groups.google.com/forum/#!searchin/docker-user/1.6.1/docker-user/47GZrihtr-4/nwgeOOFLexIJ
- FULLDISC - 20150508 Docker 1.6.1 - Security Advisory [150507]
- MISC - http://packetstormsecurity.com/files/131835/Docker-Privilege-Escalation-Information-Disclosure.html
- SUSE - openSUSE-SU-2015:0905

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.6

CVE-2016-3697 suppress

libcontainer/user/user.go in runC before 0.1.0, as used in Docker before 1.11.2, improperly treats a numeric UID as a potential username, which allows local users to gain privileges via a numeric username in the password file in a container.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://github.com/docker/docker/issues/21436
- CONFIRM - https://github.com/opencontainers/runc/commit/69af385de62ea68e2e608335cffbb0f4aa3db091
- CONFIRM - https://github.com/opencontainers/runc/pull/708
- CONFIRM - https://github.com/opencontainers/runc/releases/tag/v0.1.0
- GENTOO - GLSA-201612-28
- REDHAT - RHSA-2016:1034
- REDHAT - RHSA-2016:2634
- SUSE - openSUSE-SU-2016:1417

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (including) 1.11.1
- ...

CVE-2017-14992 suppress

Lack of content verification in Docker-CE (Also known as Moby) versions 1.12.6-0, 1.10.3, 17.03.0, 17.03.1, 17.03.2, 17.06.0, 17.06.1, 17.06.2, 17.09.0, and earlier allows a remote attacker to cause a Denial of Service via a crafted image layer payload, aka gzip bombing.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://github.com/moby/moby/issues/35075
- MISC - https://blog.cloudpassage.com/2017/10/13/discovering-docker-cve-2017-14992/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (including) 1.10.3
- ...

CVE-2019-13139 suppress

In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the "docker build" command would be able to gain command execution. An issue exists in the way "docker build" processes remote git URLs, and results in command injection into the underlying "git clone" command, leading to code execution in the context of the user executing the "docker build" command. This occurs because git ref can be misinterpreted as a flag.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: MEDIUM (4.6)
- Vector: /AV:L/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.4)
- Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190910-0001/
- DEBIAN - DSA-4521
- MISC - https://docs.docker.com/engine/release-notes/#18094
- MISC - https://github.com/moby/moby/pull/38944
- MISC - https://staaldraad.github.io/post/2019-07-16-cve-2019-13139-docker-build/
- REDHAT - RHBA-2019:3092

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:enterprise:*:*:* versions up to (excluding) 18.09.4

CVE-2019-13509 suppress

In Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploy is run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if they resend the secret.

CWE-532 Information Exposure Through Log Files

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- BID - 109253
- BUGTRAQ - 20190910 [SECURITY] [DSA 4521-1] docker.io security update
- CONFIRM - https://security.netapp.com/advisory/ntap-20190828-0003/
- DEBIAN - DSA-4521
- FEDORA - FEDORA-2019-4bed83e978
- FEDORA - FEDORA-2019-5b54793a4a
- MISC - https://docs.docker.com/engine/release-notes/
- SUSE - openSUSE-SU-2019:2021

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (excluding) 18.09.8
- ...

CVE-2019-15752 suppress

Docker Desktop Community Edition before 2.1.0.1 allows local users to gain privileges by placing a Trojan horse docker-credential-wincred.exe file in %PROGRAMDATA%\DockerDesktop\version-bin\ as a low-privilege user, and then waiting for an admin or service user to authenticate with Docker, restart Docker, or run 'docker login' to force the command.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

References:
- MISC - http://packetstormsecurity.com/files/157404/Docker-Credential-Wincred.exe-Privilege-Escalation.html
- MISC - https://medium.com/@morgan.henry.roman/elevation-of-privilege-in-docker-for-windows-2fd8450b478e
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (excluding) 2.1.0.1

CVE-2019-16884 suppress

runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- FEDORA - FEDORA-2019-3fc86a518b
- FEDORA - FEDORA-2019-96946c39dd
- FEDORA - FEDORA-2019-bd4843561c
- GENTOO - GLSA-202003-21
- MISC - https://github.com/opencontainers/runc/issues/2128
- REDHAT - RHSA-2019:3940
- REDHAT - RHSA-2019:4074
- REDHAT - RHSA-2019:4269
- SUSE - openSUSE-SU-2019:2418
- SUSE - openSUSE-SU-2019:2434
- SUSE - openSUSE-SU-2020:0045
- UBUNTU - USN-4297-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:community:*:*:* versions up to (including) 19.03.2
- ...

CVE-2019-5736 suppress

runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.

CWE-78 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

CVSSv2:
- Base Score: HIGH (9.3)
- Vector: /AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (8.6)
- Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

References:
- BID - 106976
- CISCO - https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190215-runc
- CONFIRM - https://security.netapp.com/advisory/ntap-20190307-0008/
- CONFIRM - https://softwaresupport.softwaregrp.com/document/-/facetsearch/document/KM03410944
- CONFIRM - https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03913en_us
- CONFIRM - https://support.mesosphere.com/s/article/Known-Issue-Container-Runtime-Vulnerability-MSPH-2019-0003
- CONFIRM - https://www.synology.com/security/advisory/Synology_SA_19_06
- EXPLOIT-DB - 46359
- EXPLOIT-DB - 46369
- FEDORA - FEDORA-2019-2baa1f7b19
- FEDORA - FEDORA-2019-6174b47003
- FEDORA - FEDORA-2019-bc70b381ad
- FEDORA - FEDORA-2019-c1dac1b3b8
- GENTOO - GLSA-202003-21
- MISC - https://access.redhat.com/security/cve/cve-2019-5736
- MISC - https://access.redhat.com/security/vulnerabilities/runcescape
- MISC - https://aws.amazon.com/security/security-bulletins/AWS-2019-002/
- MISC - https://azure.microsoft.com/en-us/updates/cve-2019-5736-and-runc-vulnerability/
- MISC - https://azure.microsoft.com/en-us/updates/iot-edge-fix-cve-2019-5736/
- MISC - https://blog.dragonsector.pl/2019/02/cve-2019-5736-escape-from-docker-and.html
- MISC - https://brauner.github.io/2019/02/12/privileged-containers.html
- MISC - https://bugzilla.suse.com/show_bug.cgi?id=1121967
- MISC - https://cloud.google.com/kubernetes-engine/docs/security-bulletins#february-11-2019-runc
- MISC - https://github.com/Frichetten/CVE-2019-5736-PoC
- MISC - https://github.com/docker/docker-ce/releases/tag/v18.09.2
- MISC - https://github.com/opencontainers/runc/commit/0a8e4117e7f715d5fbeef398405813ce8e88558b
- MISC - https://github.com/opencontainers/runc/commit/6635b4f0c6af3810594d2770f662f34ddc15b40d
- MISC - https://github.com/q3k/cve-2019-5736-poc
- MISC - https://github.com/rancher/runc-cve
- MISC - https://kubernetes.io/blog/2019/02/11/runc-and-cve-2019-5736/
- MISC - https://www.openwall.com/lists/oss-security/2019/02/11/2
- MISC - https://www.twistlock.com/2019/02/11/how-to-mitigate-cve-2019-5736-in-runc-and-docker/
- MLIST - [dlab-dev] 20190524 [jira] [Created] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190524 [jira] [Updated] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20190923 [jira] [Assigned] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [dlab-dev] 20200525 [jira] [Deleted] (DLAB-723) Runc vulnerability CVE-2019-5736
- MLIST - [geode-issues] 20200831 [jira] [Created] (GEODE-8471) Dependency security issues in geode-core-1.12
- MLIST - [mesos-dev] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [mesos-user] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190323 CVE-2019-0204: Some Mesos components can be overwritten making arbitrary code execution possible.
- MLIST - [oss-security] 20190628 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft

- MLIST - [oss-security] 20190706 Re: linux-distros membership application - Microsoft
- MLIST - [oss-security] 20191023 Membership application for linux-distros - VMware
- MLIST - [oss-security] 20191029 Re: Membership application for linux-distros - VMware
- REDHAT - RHSA-2019:0303
- REDHAT - RHSA-2019:0304
- REDHAT - RHSA-2019:0401
- REDHAT - RHSA-2019:0408
- REDHAT - RHSA-2019:0975
- SUSE - openSUSE-SU-2019:1079
- SUSE - openSUSE-SU-2019:1227
- SUSE - openSUSE-SU-2019:1275
- SUSE - openSUSE-SU-2019:1444
- SUSE - openSUSE-SU-2019:1481
- SUSE - openSUSE-SU-2019:1499
- SUSE - openSUSE-SU-2019:1506
- SUSE - openSUSE-SU-2019:2021
- SUSE - openSUSE-SU-2019:2245
- SUSE - openSUSE-SU-2019:2286
- UBUNTU - USN-4048-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 18.09.2
- ...

CVE-2020-27534 suppress

util/binfmt_misc/check.go in Builder in Docker Engine before 19.03.9 calls os.OpenFile with a potentially unsafe qemu-check temporary pathname, constructed with an empty first argument in an ioutil.TempDir call.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - http://web.archive.org/web/20200530054359/https://docs.docker.com/engine/release-notes/
- MISC - https://github.com/moby/buildkit/pull/1462
- MISC - https://github.com/moby/moby/pull/40877
- MISC - https://golang.org/pkg/io/ioutil/#TempDir
- MISC - https://golang.org/pkg/os/#TempDir

Vulnerable Software & Versions:

- cpe:2.3:a:docker:docker:*:*:*:*:*:*:*:* versions up to (excluding) 19.03.9

github.com/go-sql-driver/mysql:1.5.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/go-sql-driver/mysql/1.5.0

Evidence

Identifiers

- pkg:golang/github.com/go-sql-driver/mysql@1.5.0 (*Confidence*:Highest)
- cpe:2.3:a:mysql:mysql:1.5.0:*:*:*:*:*:*:* (*Confidence*:High) suppress

Published Vulnerabilities

CVE-2007-1420 suppress

MySQL 5.x before 5.0.36 allows local users to cause a denial of service (database crash) by performing information_schema table subselects and using ORDER BY to sort a single-row result, which prevents certain structure elements from being initialized and triggers a NULL dereference in the filesort function.

NVD-CWE-Other

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:N/I:N/A:P

References:
- BID - 22900
- BUGTRAQ - 20070309 SEC Consult SA-20070309-0 :: MySQL 5 Single Row Subselect Denial of Service
- CONFIRM - http://bugs.mysql.com/bug.php?id=24630
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/releasenotes-es-5-0-36.html
- CONFIRM - https://issues.rpath.com/browse/RPL-1127
- GENTOO - GLSA-200705-11
- MANDRIVA - MDKSA-2007:139
- MISC - http://www.sec-consult.com/284.html
- OVAL - oval:org.mitre.oval:def:9530
- REDHAT - RHSA-2008:0364
- SECTRACK - 1017746
- SECUNIA - 24483
- SECUNIA - 24609
- SECUNIA - 25196
- SECUNIA - 25389
- SECUNIA - 25946
- SECUNIA - 30351
- SREASON - 2413
- UBUNTU - USN-440-1
- VUPEN - ADV-2007-0908

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.0.33
- ...

CVE-2007-2583 suppress

The in_decimal::set function in item_cmpfunc.cc in MySQL before 5.0.40, and 5.1 before 5.1.18-beta, allows context-dependent attackers to cause a denial of service (crash) via a crafted IF clause that results in a divide-by-zero error and a NULL pointer dereference.

CWE-189 Numeric Errors

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:
- BID - 23911
- CONFIRM - http://bugs.mysql.com/bug.php?id=27513
- CONFIRM - http://lists.mysql.com/commits/23685
- CONFIRM - https://issues.rpath.com/browse/RPL-1356
- DEBIAN - DSA-1413
- EXPLOIT-DB - 30020

- GENTOO - GLSA-200705-11
- MANDRIVA - MDKSA-2007:139
- MISC - http://packetstormsecurity.com/files/124295/MySQL-5.0.x-Denial-Of-Service.html
- OSVDB - 34734
- OVAL - oval:org.mitre.oval:def:9930
- REDHAT - RHSA-2008:0364
- SECUNIA - 25188
- SECUNIA - 25196
- SECUNIA - 25255
- SECUNIA - 25389
- SECUNIA - 25946
- SECUNIA - 27155
- SECUNIA - 27823
- SECUNIA - 28838
- SECUNIA - 30351
- SUSE - SUSE-SR:2008:003
- TRUSTIX - 2007-0017
- UBUNTU - USN-528-1
- VUPEN - ADV-2007-1731
- XF - mysql-if-dos(34232)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.0.38
- ...

CVE-2007-2691 suppress

MySQL before 4.1.23, 5.0.x before 5.0.42, and 5.1.x before 5.1.18 does not require the DROP privilege for RENAME TABLE statements, which allows remote authenticated users to rename arbitrary tables. The vendor has released a product update to address this issue:
Upgrade to MySQL version 5.1.18: http://dev.mysql.com/downloads/

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:P

References:
- APPLE - APPLE-SA-2008-10-09
- BID - 24016
- BID - 31681
- BUGTRAQ - 20070717 rPSA-2007-0143-1 mysql mysql-bench mysql-server
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-18.html
- CONFIRM - http://support.apple.com/kb/HT3216
- CONFIRM - https://issues.rpath.com/browse/RPL-1536
- DEBIAN - DSA-1413
- MANDRIVA - MDKSA-2007:139
- MISC - http://bugs.mysql.com/bug.php?id=27515
- MLIST - [announce] 20070712 MySQL Community Server 5.0.45 has been released!
- OSVDB - 34766
- OVAL - oval:org.mitre.oval:def:9559
- REDHAT - RHSA-2007:0894
- REDHAT - RHSA-2008:0364
- REDHAT - RHSA-2008:0768
- SECTRACK - 1018069
- SECUNIA - 25301
- SECUNIA - 25946
- SECUNIA - 26073
- SECUNIA - 26430
- SECUNIA - 27155
- SECUNIA - 27823
- SECUNIA - 28838
- SECUNIA - 30351
- SECUNIA - 31226
- SECUNIA - 32222
- SUSE - SUSE-SR:2008:003
- UBUNTU - USN-528-1
- VUPEN - ADV-2007-1804
- VUPEN - ADV-2008-2780
- XF - mysql-renametable-weak-security(34347)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 4.1.22
- ...

CVE-2007-5925 suppress

The convert_search_mode_to_innobase function in ha_innodb.cc in the InnoDB engine in MySQL 5.1.23-BK and earlier allows remote authenticated users to cause a denial of service (database crash) via a certain CONTAINS operation on an indexed column, which triggers an assertion error.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:
- BID - 26353
- CONFIRM - http://bugs.gentoo.org/show_bug.cgi?id=198988
- CONFIRM - http://bugs.mysql.com/bug.php?id=32125
- DEBIAN - DSA-1413
- FEDORA - FEDORA-2007-4465
- FEDORA - FEDORA-2007-4471
- FULLDISC - 20071106 MySQL 5.x DoS (unknown)
- GENTOO - GLSA-200711-25
- MANDRIVA - MDKSA-2007:243
- OVAL - oval:org.mitre.oval:def:11390
- REDHAT - RHSA-2007:1155
- REDHAT - RHSA-2007:1157
- SECTRACK - 1018978
- SECUNIA - 27568
- SECUNIA - 27649
- SECUNIA - 27823
- SECUNIA - 28025
- SECUNIA - 28040
- SECUNIA - 28099
- SECUNIA - 28108
- SECUNIA - 28128
- SECUNIA - 28838
- SLACKWARE - SSA:2007-348-01
- SUSE - SUSE-SR:2008:003
- UBUNTU - USN-1397-1
- UBUNTU - USN-559-1
- VUPEN - ADV-2007-3903
- XF - mysql-hainnodb-dos(38284)

Vulnerable Software & Versions:

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.23_bk

CVE-2009-0819 suppress

sql/item_xmlfunc.cc in MySQL 5.1 before 5.1.32 and 6.0 before 6.0.10 allows remote authenticated users to cause a denial of service (crash) via "an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML()," which triggers an assertion failure.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:
- BID - 33972
- CONFIRM - http://bugs.mysql.com/bug.php?id=42495
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-32.html
- CONFIRM - http://dev.mysql.com/doc/refman/6.0/en/news-6-0-10.html
- OVAL - oval:org.mitre.oval:def:7544
- SECTRACK - 1021786
- SECUNIA - 34115
- VUPEN - ADV-2009-0594
- XF - mysql-xpath-dos(49050)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.32-bzr
- ...

CVE-2009-4028 suppress

The vio_verify_callback function in viosslfactories.c in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41, when OpenSSL is used, accepts a value of zero for the depth of X.509 certificates, which allows man-in-the-middle attackers to spoof arbitrary SSL-based MySQL servers via a crafted certificate, as demonstrated by a certificate presented by a server linked against the yaSSL library.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- CONFIRM - http://bugs.mysql.com/47320
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-88.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html
- MLIST - [commits] 20091020 bzr commit into mysql-4.1 branch (joro:2709) Bug#47320
- MLIST - [oss-security] 20091119 mysql-5.1.41
- MLIST - [oss-security] 20091121 CVE Request - MySQL - 5.0.88
- MLIST - [oss-security] 20091123 Re: mysql-5.1.41
- OVAL - oval:org.mitre.oval:def:10940
- OVAL - oval:org.mitre.oval:def:8510
- REDHAT - RHSA-2010:0109
- SUSE - SUSE-SR:2010:011
- VUPEN - ADV-2010-1107

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.0.87
- ...

CVE-2010-1621 suppress

The mysql_uninstall_plugin function in sql/sql_plugin.cc in MySQL 5.1 before 5.1.46 does not check privileges before uninstalling a plugin, which allows remote attackers to uninstall arbitrary plugins via the UNINSTALL PLUGIN command.

CWE-264 Permissions, Privileges, and Access Controls

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

References:
- BID - 39543
- CONFIRM - http://bugs.mysql.com/bug.php?id=51770
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-46.html
- MANDRIVA - MDVSA-2010:093
- UBUNTU - USN-1397-1

Vulnerable Software & Versions:

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.45

CVE-2010-1626 suppress

MySQL before 5.1.46 allows local users to delete the data and index files of another user's MyISAM table via a symlink attack in conjunction with the DROP TABLE command, a different vulnerability than CVE-2008-4098 and CVE-2008-7247.

CWE-264 Permissions, Privileges, and Access Controls, CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:
- Base Score: LOW (3.6)
- Vector: /AV:L/AC:L/Au:N/C:N/I:P/A:P

References:
- BID - 40257
- CONFIRM - http://bugs.mysql.com/bug.php?id=40980
- MANDRIVA - MDVSA-2010:101
- MLIST - [oss-security] 20100510 Re: A mysql flaw.
- MLIST - [oss-security] 20100518 Re: A mysql flaw.
- OVAL - oval:org.mitre.oval:def:9490
- REDHAT - RHSA-2010:0442
- SECTRACK - 1024004
- SUSE - SUSE-SR:2010:019
- SUSE - SUSE-SR:2010:021
- UBUNTU - USN-1397-1
- VUPEN - ADV-2010-1194

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.45
- ...

CVE-2010-3677 suppress

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) via a join query that uses a table with a unique SET column.

CWE-399 Resource Management Errors

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:
- APPLE - APPLE-SA-2011-06-23-1
- BID - 42646
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
- CONFIRM - http://support.apple.com/kb/HT4723
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=628040
- DEBIAN - DSA-2143
- MANDRIVA - MDVSA-2010:155
- MANDRIVA - MDVSA-2010:222
- MANDRIVA - MDVSA-2011:012
- MISC - http://bugs.mysql.com/bug.php?id=54575
- MLIST - [oss-security] 20100928 Re: CVE Request -- MySQL v5.1.49 -- multiple DoS flaws
- REDHAT - RHSA-2010:0825
- REDHAT - RHSA-2011:0164
- SECUNIA - 42875
- SECUNIA - 42936
- SUSE - SUSE-SR:2010:019
- TURBO - TLSA-2011-3
- UBUNTU - USN-1017-1
- UBUNTU - USN-1397-1
- VUPEN - ADV-2011-0105
- VUPEN - ADV-2011-0133
- VUPEN - ADV-2011-0170

- VUPEN - ADV-2011-0345
- XF - mysql-setcolumn-dos(64688)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.48
- ...

CVE-2010-3682 suppress

Oracle MySQL 5.1 before 5.1.49 and 5.0 before 5.0.92 allows remote authenticated users to cause a denial of service (mysqld daemon crash) by using EXPLAIN with crafted "SELECT ... UNION ... ORDER BY (SELECT ... WHERE ...)" statements, which triggers a NULL pointer dereference in the Item_singlerow_subselect::store function. Per: http://cwe.mitre.org/data/definitions/476.html

'CWE-476: NULL Pointer Dereference'

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

References:
- APPLE - APPLE-SA-2011-06-23-1
- BID - 42599
- CONFIRM - http://bugs.mysql.com/bug.php?id=52711
- CONFIRM - http://dev.mysql.com/doc/refman/5.0/en/news-5-0-92.html
- CONFIRM - http://dev.mysql.com/doc/refman/5.1/en/news-5-1-49.html
- CONFIRM - http://support.apple.com/kb/HT4723
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=628328
- DEBIAN - DSA-2143
- MANDRIVA - MDVSA-2010:155
- MANDRIVA - MDVSA-2010:222
- MANDRIVA - MDVSA-2011:012
- MLIST - [oss-security] 20100928 Re: CVE Request -- MySQL v5.1.49 -- multiple DoS flaws
- REDHAT - RHSA-2010:0825
- REDHAT - RHSA-2011:0164
- SECUNIA - 42875
- SECUNIA - 42936
- SUSE - SUSE-SR:2010:019
- TURBO - TLSA-2011-3
- UBUNTU - USN-1017-1
- UBUNTU - USN-1397-1
- VUPEN - ADV-2011-0105
- VUPEN - ADV-2011-0133
- VUPEN - ADV-2011-0170
- VUPEN - ADV-2011-0345
- XF - mysql-itemsinglerowsubselect-dos(64684)

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.48
- ...

CVE-2012-5627 suppress

Oracle MySQL and MariaDB 5.5.x before 5.5.29, 5.3.x before 5.3.12, and 5.2.x before 5.2.14 does not modify the salt during multiple executions of the change_user command within the same connection which makes it easier for remote authenticated users to conduct brute force password guessing attacks.

CWE-255 Credentials Management

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

References:
- CONFIRM - https://mariadb.atlassian.net/browse/MDEV-3915
- FULLDISC - 20121203 MySQL Local/Remote FAST Account Password Cracking
- FULLDISC - 20121205 Re: MySQL Local/Remote FAST Account Password Cracking
- GENTOO - GLSA-201308-06
- MANDRIVA - MDVSA-2013:102
- MISC - https://bugzilla.redhat.com/show_bug.cgi?id=883719
- MLIST - [oss-security] 20121206 Re: CVE request: Mysql/Mariadb insecure salt-usage
- SECUNIA - 53372

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:*
- ...

CVE-2015-2575 suppress

Unspecified vulnerability in the MySQL Connectors component in Oracle MySQL 5.1.34 and earlier allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Connector/J.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:N

References:
- BID - 74075
- CONFIRM - http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
- CONFIRM - https://security.netapp.com/advisory/ntap-20150417-0003/
- DEBIAN - DSA-3621
- SECTRACK - 1032121
- SUSE - SUSE-SU-2015:0946
- SUSE - openSUSE-SU-2015:0967

Vulnerable Software & Versions:

- cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:* versions up to (including) 5.1.34

CVE-2017-15945 suppress

The installation scripts in the Gentoo dev-db/mysql, dev-db/mariadb, dev-db/percona-server, dev-db/mysql-cluster, and dev-db/mariadb-galera packages before 2017-09-29 have chown calls for user-writable directory trees, which allows local users to gain privileges by leveraging access to the mysql account for creation of a link.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: HIGH (7.2)
- Vector: /AV:L/AC:L/Au:N/C:C/I:C/A:C

CVSSv3:
- Base Score: HIGH (7.8)
- Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://bugs.gentoo.org/630822
- GENTOO - GLSA-201711-04

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:mysql:mysql:*:r1:*:*:*:*:*:* versions up to (excluding) 5.6.36
- ...

github.com/grpc-ecosystem/go-grpc-middleware:1.2.0

License:

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with

File Path: /Users/akhode/go/pkg/mod/github.com/grpc-ecosystem/go-grpc-middleware@v1.2.0

Evidence

Identifiers

- pkg:golang/github.com/grpc-ecosystem/go-grpc-middleware@1.2.0 (*Confidence*:Highest)
- cpe:2.3:a:grpc:grpc:1.2.0:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2017-8359 suppress

Google gRPC before 2017-03-29 has an out-of-bounds write caused by a heap-based use-after-free related to the grpc_call_destroy function in core/lib/surface/call.c.

CWE-787 Out-of-bounds Write

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- BID - 98280
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=726
- MISC - https://github.com/grpc/grpc/pull/10353

Vulnerable Software & Versions:

- cpe:2.3:a:grpc:grpc:*:*:*:*:*:*:*:* versions up to (including) 1.2.1

CVE-2017-9431 suppress

Google gRPC before 2017-04-05 has an out-of-bounds write caused by a heap-based buffer overflow related to core/lib/iomgr/error.c.

CWE-787 Out-of-bounds Write

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=1018

- MISC - https://github.com/grpc/grpc/pull/10492

Vulnerable Software & Versions:

- cpe:2.3:a:grpc:grpc:*:*:*:*:*:*:*:* versions up to (including) 1.2.2

CVE-2020-7768 suppress

The package grpc before 1.24.4; the package @grpc/grpc-js before 1.1.8 are vulnerable to Prototype Pollution via loadPackageDefinition.

CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://github.com/grpc/grpc-node/pull/1605
- MISC - https://github.com/grpc/grpc-node/pull/1606
- MISC - https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1038819
- MISC - https://snyk.io/vuln/SNYK-JS-GRPC-598671
- MISC - https://snyk.io/vuln/SNYK-JS-GRPCGRPCJS-1038818

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:grpc:grpc:*:*:*:*:*:-:*:* versions up to (excluding) 1.24.2
- ...

github.com/grpc-ecosystem/grpc-gateway:1.14.3

License:

Copyright (c) 2015, Gengo, Inc.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice,
  this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name of Gengo, Inc. nor the names of its
  contributors may be used to endorse or promote products derived from this
  software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

File Path: /Users/akhode/go/pkg/mod/github.com/grpc-ecosystem/grpc-gateway@v1.14.3

Evidence

Identifiers

- pkg:golang/github.com/grpc-ecosystem/grpc-gateway@1.14.3 (*Confidence*:Highest)
- cpe:2.3:a:grpc:grpc:1.14.3:*:*:*:*:*:*:* (*Confidence*:Highest) suppress

Published Vulnerabilities

CVE-2020-7768 suppress

The package grpc before 1.24.4; the package @grpc/grpc-js before 1.1.8 are vulnerable to Prototype Pollution via loadPackageDefinition.

CWE-74 Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://github.com/grpc/grpc-node/pull/1605
- MISC - https://github.com/grpc/grpc-node/pull/1606
- MISC - https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1038819
- MISC - https://snyk.io/vuln/SNYK-JS-GRPC-598671
- MISC - https://snyk.io/vuln/SNYK-JS-GRPCGRPCJS-1038818

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:grpc:grpc:*:*:*:*:*:-:*:* versions up to (excluding) 1.24.2
- ...

github.com/prometheus/client_golang:0.9.3-0.20190127221311-3c4408c8b829

File Path: /Users/akhode/v4/dss/go.mod:github.com/prometheus/client_golang/0.9.3-0.20190127221311-3c4408c8b829

Evidence

Identifiers

- pkg:golang/github.com/prometheus/client_golang@0.9.3-0.20190127221311-3c4408c8b829 (*Confidence*:Highest)
- cpe:2.3:a:prometheus:prometheus:0.9.3.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2019-3826 suppress

A stored, DOM based, cross-site scripting (XSS) flaw was found in Prometheus before version 2.7.1. An attacker could exploit this by convincing an authenticated user to visit a crafted URL on a Prometheus server, allowing for the execution and persistent storage of arbitrary scripts.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3826
- CONFIRM - https://github.com/prometheus/prometheus/commit/62e591f9
- CONFIRM - https://github.com/prometheus/prometheus/pull/5163
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch master updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- REDHAT - RHBA-2019:0327

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:prometheus:prometheus:*:*:*:*:*:*:*:* versions up to (excluding) 2.7.1
- ...

github.com/prometheus/client_model:0.0.0-20190812154241-14fe0d1b01d4

File Path: /Users/akhode/v4/dss/go.mod:github.com/prometheus/client_model/0.0.0-20190812154241-14fe0d1b01d4

Evidence

Identifiers

- pkg:golang/github.com/prometheus/client_model@0.0.0-20190812154241-14fe0d1b01d4 (*Confidence*:Highest)
- cpe:2.3:a:prometheus:prometheus:0.0.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2019-3826 suppress

A stored, DOM based, cross-site scripting (XSS) flaw was found in Prometheus before version 2.7.1. An attacker could exploit this by convincing an authenticated user to visit a crafted URL on a Prometheus server, allowing for the execution and persistent storage of arbitrary scripts.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3826
- CONFIRM - https://github.com/prometheus/prometheus/commit/62e591f9
- CONFIRM - https://github.com/prometheus/prometheus/pull/5163
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch master updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- REDHAT - RHBA-2019:0327

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:prometheus:prometheus:*:*:*:*:*:*:*:* versions up to (excluding) 2.7.1
- ...

github.com/prometheus/common:0.2.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/prometheus/common/0.2.0

Evidence

Identifiers

- pkg:golang/github.com/prometheus/common@0.2.0 (*Confidence*:Highest)
- cpe:2.3:a:prometheus:prometheus:0.2.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2019-3826 suppress

A stored, DOM based, cross-site scripting (XSS) flaw was found in Prometheus before version 2.7.1. An attacker could exploit this by convincing an authenticated user to visit a crafted URL on a Prometheus server, allowing for the execution and persistent storage of arbitrary scripts.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)

- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3826
- CONFIRM - https://github.com/prometheus/prometheus/commit/62e591f9
- CONFIRM - https://github.com/prometheus/prometheus/pull/5163
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch master updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- REDHAT - RHBA-2019:0327

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:prometheus:prometheus:*:*:*:*:*:*:*:* versions up to (excluding) 2.7.1
- ...

github.com/prometheus/procfs:0.0.0-20190117184657-bf6a532e95b1

File Path: /Users/akhode/v4/dss/go.mod:github.com/prometheus/procfs/0.0.0-20190117184657-bf6a532e95b1

Evidence

Identifiers

- pkg:golang/github.com/prometheus/procfs@0.0.0-20190117184657-bf6a532e95b1 (*Confidence*:Highest)
- cpe:2.3:a:prometheus:prometheus:0.0.0:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2019-3826 suppress

A stored, DOM based, cross-site scripting (XSS) flaw was found in Prometheus before version 2.7.1. An attacker could exploit this by convincing an authenticated user to visit a crafted URL on a Prometheus server, allowing for the execution and persistent storage of arbitrary scripts.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3826
- CONFIRM - https://github.com/prometheus/prometheus/commit/62e591f9
- CONFIRM - https://github.com/prometheus/prometheus/pull/5163
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.5 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch branch-3.6 updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- MLIST - [zookeeper-commits] 20200118 [zookeeper] branch master updated: ZOOKEEPER-3677: owasp checker failing for - CVE-2019-17571 Apache Log4j 1.2 deserialization of untrusted data in SocketServer
- REDHAT - RHBA-2019:0327

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:prometheus:prometheus:*:*:*:*:*:*:*:* versions up to (excluding) 2.7.1
- ...

github.com/robfig/cron/v3:3.0.1

License:

Copyright (C) 2012 Rob Figueiredo
All Rights Reserved.

MIT LICENSE

Permission is hereby granted, free of charge, to any person obtaining a copy of
this software and associated documentation files (the "Software"), to deal in
the Software without restriction, including without limitation the rights to
use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software is furnished to do so,
subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS
FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR
COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER
IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN
CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

File Path: /Users/akhode/go/pkg/mod/github.com/robfig/cron/v3@v3.0.1

Evidence

Identifiers

- pkg:golang/github.com/robfig/cron/v3@3.0.1 (*Confidence*:Highest)
- cpe:2.3:a:cron_project:cron:3.0.1:*:*:*:*:*:*:* (*Confidence*:Low) suppress

Published Vulnerabilities

CVE-2017-9525 suppress

In the cron package through 3.0pl1-128 on Debian, and through 3.0pl1-128ubuntu2 on Ubuntu, the postinst maintainer script allows for group-crontab-to-root privilege escalation via symlink attacks against unsafe usage of the chown and chmod programs.

CWE-59 Improper Link Resolution Before File Access ('Link Following')

CVSSv2:
- Base Score: MEDIUM (6.9)
- Vector: /AV:L/AC:M/Au:N/C:C/I:C/A:C

CVSSv3:

- Base Score: MEDIUM (6.7)
- Vector: CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - http://bugs.debian.org/864466
- MISC - http://www.openwall.com/lists/oss-security/2017/06/08/3
- MLIST - [debian-lts-announce] 20190321 [SECURITY] [DLA 1723-1] cron security update
- SECTRACK - 1038651

Vulnerable Software & Versions:

- cpe:2.3:a:cron_project:cron:*:*:*:*:*:*:*:* versions up to (including) 3.0pl1-128.

CVE-2019-9704 suppress

Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (daemon crash) via a large crontab file because the calloc return value is not checked.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- BID - 107373
- FEDORA - FEDORA-2019-7104a00054
- MISC - https://salsa.debian.org/debian/cron/commit/f2525567
- MLIST - [debian-lts-announce] 20190321 [SECURITY] [DLA 1723-1] cron security update

Vulnerable Software & Versions:

- cpe:2.3:a:cron_project:cron:*:*:*:*:*:*:*:* versions up to (excluding) 3.0pl1-133

CVE-2019-9705 suppress

Vixie Cron before the 3.0pl1-133 Debian package allows local users to cause a denial of service (memory consumption) via a large crontab file because an unlimited number of lines is accepted.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- BID - 107378
- FEDORA - FEDORA-2019-7104a00054
- MISC - https://salsa.debian.org/debian/cron/commit/26814a26
- MLIST - [debian-lts-announce] 20190321 [SECURITY] [DLA 1723-1] cron security update

Vulnerable Software & Versions:

- cpe:2.3:a:cron_project:cron:*:*:*:*:*:*:*:* versions up to (excluding) 3.0pl1-133

github.com/xanzy/go-gitlab:0.15.0

File Path: /Users/akhode/v4/dss/go.mod:github.com/xanzy/go-gitlab/0.15.0

Evidence

Identifiers

- pkg:golang/github.com/xanzy/go-gitlab@0.15.0 (*Confidence*:Highest)
- cpe:2.3:a:gitlab:gitlab:0.15.0:*:*:*:*:*:*:* (*Confidence*:High) suppress

Published Vulnerabilities

CVE-2013-4580 suppress

GitLab before 5.4.2, Community Edition before 6.2.4, and Enterprise Edition before 6.2.1, when using a MySQL backend, allows remote attackers to impersonate arbitrary users and bypass authentication via unspecified API calls.

CWE-287 Improper Authentication

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- CONFIRM - https://www.gitlab.com/2013/11/14/multiple-critical-vulnerabilities-in-gitlab/
- MLIST - [oss-security] 20131114 Re: Requesting four (4) CVE identifiers for GitLab

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 6.2.3
- ...

CVE-2013-4581 suppress

GitLab 5.0 before 5.4.2, Community Edition before 6.2.4, Enterprise Edition before 6.2.1 and gitlab-shell before 1.7.8 allows remote attackers to execute arbitrary code via a crafted change using SSH.

CWE-94 Improper Control of Generation of Code ('Code Injection')

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

References:
- CONFIRM - https://www.gitlab.com/2013/11/14/multiple-critical-vulnerabilities-in-gitlab/
- MLIST - [oss-security] 20131114 Re: Requesting four (4) CVE identifiers for GitLab

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 6.2.3
- ...

CVE-2017-0919 suppress

GitLab Community and Enterprise Editions before 10.1.6, 10.2.6, and 10.3.4 are vulnerable to an authorization bypass issue in the GitLab import component resulting in an attacker being able to perform operations under a group in which they were previously unauthorized.

CWE-306 Missing Authentication for Critical Function

CVSSv2:

- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://hackerone.com/reports/301137

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 10.1.6
- ...

CVE-2017-0921 suppress

GitLab Community and Enterprise Editions before 10.1.6, 10.2.6, and 10.3.4 are vulnerable to an unverified password change issue in the PasswordsController component resulting in potential account takeover if a victim's session is compromised.

CWE-640 Weak Password Recovery Mechanism for Forgotten Password

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://about.gitlab.com/2018/05/29/security-release-gitlab-10-dot-8-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 10.1.6
- ...

CVE-2017-12426 suppress

GitLab Community Edition (CE) and Enterprise Edition (EE) before 8.17.8, 9.0.x before 9.0.13, 9.1.x before 9.1.10, 9.2.x before 9.2.10, 9.3.x before 9.3.10, and 9.4.x before 9.4.4 might allow remote attackers to execute arbitrary code via a crafted SSH URL in a project import.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://about.gitlab.com/2017/08/10/gitlab-9-dot-4-dot-4-released/
- MLIST - [linux-kernel] 20170810 [ANNOUNCE] Git v2.14.1, v2.13.5, and others

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (including) 8.17.7
- ...

CVE-2017-8778 suppress

GitLab before 8.14.9, 8.15.x before 8.15.6, and 8.16.x before 8.16.5 has XSS via a SCRIPT element in an issue attachment or avatar that is an SVG document.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2017/02/15/gitlab-8-dot-16-dot-5-security-release/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/27471

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (including) 8.14.9
- ...

CVE-2018-10379 suppress

An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 10.5.8, 10.6.x before 10.6.5, and 10.7.x before 10.7.2. The Move Issue feature contained a persistent XSS vulnerability.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- BID - 104491
- CONFIRM - https://about.gitlab.com/2018/04/30/security-release-gitlab-10-dot-7-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.5.8
- ...

CVE-2018-12606 suppress

An issue was discovered in GitLab Community Edition and Enterprise Edition before 10.7.6, 10.8.x before 10.8.5, and 11.x before 11.0.1. The wiki contains a persistent XSS issue due to a lack of output encoding affecting a specific markdown feature.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/06/25/security-release-gitlab-11-dot-0-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/46957

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.7.6
- ...

CVE-2018-12607 suppress

An issue was discovered in GitLab Community Edition and Enterprise Edition before 10.7.6, 10.8.x before 10.8.5, and 11.x before 11.0.1. The charts feature contained a persistent XSS issue due to a lack of output encoding.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/06/25/security-release-gitlab-11-dot-0-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/45903

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.7.6
- ...

CVE-2018-14364 suppress

GitLab Community and Enterprise Edition before 10.7.7, 10.8.x before 10.8.6, and 11.x before 11.0.4 allows Directory Traversal with write access and resultant remote code execution via the GitLab projects import component.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://about.gitlab.com/2018/07/17/critical-security-release-gitlab-11-dot-0-dot-4-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/49133
- MISC - https://hackerone.com/reports/378148

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 10.7.7
- ...

CVE-2018-14602 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. Information Disclosure can occur because the Prometheus metrics feature discloses private project pathnames.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-com/infrastructure/issues/4423
- MISC - https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.8.7
- ...

CVE-2018-14603 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. CSRF can occur in the Test feature of the System Hooks component.

CWE-352 Cross-Site Request Forgery (CSRF)

CVSSv2:
- Base Score: MEDIUM (6.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

References:
- MISC - https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.8.7
- ...

CVE-2018-14604 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the tooltip of the job inside the CI/CD pipeline.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.8.7
- ...

CVE-2018-14605 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur in the branch name during a Web IDE file commit.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/47793
- MISC - https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.8.7
- ...

CVE-2018-14606 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 10.8.7, 11.0.x before 11.0.5, and 11.1.x before 11.1.2. XSS can occur via a Milestone name during a promotion.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/48617
- MISC - https://about.gitlab.com/2018/07/26/security-release-gitlab-11-dot-1-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 10.8.7
- ...

CVE-2018-18640 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It has Information Exposure Through Browser Caching.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/10/29/security-release-gitlab-11-dot-4-dot-3-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/51423

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.2.7
- ...

CVE-2018-18643 suppress

GitLab CE & EE 11.2 and later and before 11.5.0-rc12, 11.4.6, and 11.3.10 have Persistent XSS.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://about.gitlab.com/2018/11/19/critical-security-release-gitlab-11-dot-4-dot-6-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/53385

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 11.2.0
- ...

CVE-2018-18645 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.2.7, 11.3.x before 11.3.8, and 11.4.x before 11.4.3. It allows for Information Exposure via unsubscribe links in email replies.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/10/29/security-release-gitlab-11-dot-4-dot-3-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/24498

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.2.7
- ...

CVE-2018-19495 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.3.11, 11.4.x before 11.4.8, and 11.5.x before 11.5.1. There is an SSRF vulnerability in the Prometheus integration.

CWE-918 Server-Side Request Forgery (SSRF)

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/11/28/security-release-gitlab-11-dot-5-dot-1-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ee/issues/8167

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.3.11
- ...

CVE-2018-19580 suppress

All versions of GitLab prior to 11.5.1, 11.4.8, and 11.3.11 do not send an email to the old email address when an email address change is made.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/11/28/security-release-gitlab-11-dot-5-dot-1-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/39809

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.3.11

- ...

CVE-2018-19856 suppress

GitLab CE/EE before 11.3.12, 11.4.x before 11.4.10, and 11.5.x before 11.5.3 allows Directory Traversal in Templates API.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2018/12/06/critical-security-release-gitlab-11-dot-5-dot-3-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/54857

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.3.12
- ...

CVE-2018-20229 suppress

GitLab Community and Enterprise Edition before 11.3.14, 11.4.x before 11.4.12, and 11.5.x before 11.5.5 allows Directory Traversal.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2018/12/20/critical-security-release-gitlab-11-dot-5-dot-5-released/
- CONFIRM - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.3.14
- ...

CVE-2018-8971 suppress

The Auth0 integration in GitLab before 10.3.9, 10.4.x before 10.4.6, and 10.5.x before 10.5.6 has an incorrect omniauth-auth0 configuration, leading to signing in unintended users.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- DEBIAN - DSA-4206
- MISC - https://about.gitlab.com/2018/03/20/critical-security-release-gitlab-10-dot-5-dot-6-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (including) 10.3.8
- ...

CVE-2019-10108 suppress

An Incorrect Access Control (issue 1 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. It allowed non-members of a private project/group to add and read labels.

CWE-639 Authorization Bypass Through User-Controlled Key

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/56985

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10109 suppress

An Information Exposure issue (issue 1 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. EXIF geolocation data were not removed from images when uploaded to GitLab. As a result, anyone with access to the uploaded image could obtain its geolocation, device, and software version data (if present).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/54220
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/55469

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10110 suppress

An Insecure Permissions issue (issue 1 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The "move issue" feature may allow a user to create projects under any namespace on any GitLab instance on which they hold credentials.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/56865

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10111 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. It allows persistent XSS in the merge request "resolve conflicts" page.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/56927

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10112 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The construction of the HMAC key was insecurely derived.

CWE-320 Key Management Errors

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ee/issues/9730

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10113 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. Making concurrent GET /api/v4/projects/<id>/languages requests may allow Uncontrolled Resource Consumption.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/54977

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10114 suppress

An Information Exposure issue (issue 2 of 2) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. During the OAuth authentication process, the application attempts to validate a parameter in an insecure way, potentially exposing data.

CWE-203 Information Exposure Through Discrepancy

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ee/issues/9729

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10115 suppress

An Insecure Permissions issue (issue 2 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. The GitLab Releases feature could allow guest users access to private information like release details and code information.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/56402

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10116 suppress

An Insecure Permissions issue (issue 3 of 3) was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. Guests of a project were allowed to see Related Branches created for an issue.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/56224

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10117 suppress

An Open Redirect issue was discovered in GitLab Community and Enterprise Edition before 11.7.8, 11.8.x before 11.8.4, and 11.9.x before 11.9.2. A redirect is triggered after successful authentication within the Oauth/:GeoAuthController for the secondary Geo node.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv2:
- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ee/issues/9731

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 11.7.8
- ...

CVE-2019-10640 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.7.10, 11.8.x before 11.8.6, and 11.9.x before 11.9.4. A regex input validation issue for the .gitlab-ci.yml refs value allows Uncontrolled Resource Consumption.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://about.gitlab.com/2019/04/01/security-release-gitlab-11-dot-9-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/49665

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.7.10
- ...

CVE-2019-11000 suppress

An issue was discovered in GitLab Enterprise Edition before 11.7.11, 11.8.x before 11.8.7, and 11.9.x before 11.9.7. It allows Information Disclosure.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- BID - 108301
- CONFIRM - https://about.gitlab.com/2019/04/10/critical-security-release-gitlab-11-dot-9-dot-7-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.7.11
- ...

CVE-2019-13003 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 12.0.3. One of the parsers used by Gilab CI was vulnerable to a resource exhaustion attack. It allows Uncontrolled Resource Consumption.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://about.gitlab.com/releases/2019/07/03/security-release-gitlab-12-dot-0-dot-3-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.0.3
- ...

CVE-2019-15575 suppress

A command injection exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to inject commands via the API through the blobs scope.

CWE-77 Improper Neutralization of Special Elements used in a Command ('Command Injection')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://hackerone.com/reports/682442

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.1.12
- ...

CVE-2019-15576 suppress

An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed an attacker to view private system notes from a GraphQL endpoint.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://hackerone.com/reports/633001

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.1.12
- ...

CVE-2019-15577 suppress

An information disclosure vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.12 that allowed project milestones to be disclosed via groups browsing.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://hackerone.com/reports/636560

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.1.12
- ...

CVE-2019-15580 suppress

An information exposure vulnerability exists in gitlab.com <v12.3.2, <v12.2.6, and <v12.1.10 when using the blocking merge request feature, it was possible for an unauthenticated user to see the head pipeline data of a public project even though pipeline visibility was restricted.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://hackerone.com/reports/667408

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.1.10
- ...

CVE-2019-15584 suppress

A denial of service exists in gitlab <v12.3.2, <v12.2.6, and <v12.1.10 that would let an attacker bypass input validation in markdown fields take down the affected page.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- MISC - https://hackerone.com/reports/670572

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.1.10
- ...

CVE-2019-15589 suppress

An improper access control vulnerability exists in Gitlab <v12.3.2, <v12.2.6, <v12.1.12 which would allow a blocked user would be able to use GIT clone and pull if he had obtained a CI/CD token before.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://hackerone.com/reports/497047

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.1.12
- ...

CVE-2019-15591 suppress

An improper access control vulnerability exists in GitLab <12.3.3 that allows an attacker to obtain container and dependency scanning reports through the merge request widget even though public pipelines were disabled.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://hackerone.com/reports/676976

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.3.3

- ...

CVE-2019-15592 suppress

GitLab 12.2.2 and below contains a security vulnerability that allows a guest user in a private project to see the merge request ID associated to an issue via the activity timeline.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/releases/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/
- MISC - https://hackerone.com/reports/588876

Vulnerable Software & Versions:

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:*

CVE-2019-15594 suppress

GitLab 11.8 and later contains a security vulnerability that allows a user to obtain details of restricted pipelines via the merge request endpoint.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/releases/2019/07/29/security-release-gitlab-12-dot-1-dot-2-released/
- MISC - https://hackerone.com/reports/507064

Vulnerable Software & Versions:

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (including) 11.8

CVE-2019-15726 suppress

An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Embedded images and media files in markdown could be pointed to an arbitrary server, which would reveal the IP address of clients requesting the file from that server.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/55115

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.0.8
- ...

CVE-2019-15736 suppress

An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Under certain circumstances, CI pipelines could potentially be used in a denial of service attack.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/51401

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.0.8
- ...

CVE-2019-15737 suppress

An issue was discovered in GitLab Community and Enterprise Edition through 12.2.1. Certain account actions needed improved authentication and session management.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (6.4)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/08/29/security-release-gitlab-12-dot-2-dot-3-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/42733

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.0.8
- ...

CVE-2019-18447 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Insecure Permissions.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/blog/2019/10/30/security-release-gitlab-12-dot-4-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.4.0
- ...

CVE-2019-18448 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 12.4. It has Incorrect Access Control.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/blog/2019/10/30/security-release-gitlab-12-dot-4-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.4.0
- ...

CVE-2019-18449 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 12.4 in the autocomplete feature. It has Insecure Permissions (issue 2 of 2).

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/blog/2019/10/30/security-release-gitlab-12-dot-4-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.4.0
- ...

CVE-2019-18450 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 12.4 in the Project labels feature. It has Insecure Permissions.

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/blog/2019/10/30/security-release-gitlab-12-dot-4-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.4.0
- ...

CVE-2019-18463 suppress

An issue was discovered in GitLab Community and Enterprise Edition through 12.4. It has Insecure Permissions (issue 4 of 4).

CWE-732 Incorrect Permission Assignment for Critical Resource

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://about.gitlab.com/blog/2019/10/30/security-release-gitlab-12-dot-4-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.4.0
- ...

CVE-2019-19257 suppress

GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 1 of 2).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/blog/2019/11/27/security-release-gitlab-12-5-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.5.1
- ...

CVE-2019-19260 suppress

GitLab Community Edition (CE) and Enterprise Edition (EE) through 12.5 has Incorrect Access Control (issue 2 of 2).

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/blog/2019/11/27/security-release-gitlab-12-5-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.5.1
- ...

CVE-2019-5486 suppress

A authentication bypass vulnerability exists in GitLab CE/EE <v12.3.2, <v12.2.6, and <v12.1.10 in the Salesforce login integration that could be used by an attacker to create an account that bypassed domain restrictions and email verification requirements.

CWE-287 Improper Authentication

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://hackerone.com/reports/617896

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.1.10
- ...

CVE-2019-5487 suppress

An improper access control vulnerability exists in Gitlab EE <v12.3.3, <v12.2.7, & <v12.1.13 that allowed the group search feature with Elasticsearch to return private code, merge requests and commits.

NVD-CWE-Other

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- MISC - https://hackerone.com/reports/692252

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.1.13
- ...

CVE-2019-6240 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.4. It allows Directory Traversal.

CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/01/16/critical-security-release-gitlab-11-dot-6-dot-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.4.0
- ...

CVE-2019-6781 suppress

An Improper Input Validation issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It was possible to use the profile name to inject a potentially malicious link into notification emails.

CWE-601 URL Redirection to Untrusted Site ('Open Redirect')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/22076
- MISC - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:*
- ...

CVE-2019-6784 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 1 of 2). Markdown fields contain a lack of input validation and output encoding when processing KaTeX that results in a persistent XSS.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54416

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-6791 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Incorrect Access Control (issue 3 of 3). When a project with visibility more permissive than the target group is imported, it will retain its prior visibility.

CWE-281 Improper Preservation of Permissions

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-6794 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows Information Disclosure (issue 5 of 6). A project guest user can view the last commit status of the default branch.

CWE-269 Improper Privilege Management

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54353

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-6795 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It has Insufficient Visual Distinction of Homoglyphs Presented to a User. IDN homographs and RTLO characters are rendered to unicode, which could be used for social engineering.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/29365

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-6796 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 2 of 2). The user status field contains a lack of input validation and output encoding that results in a persistent XSS.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/55320
- MISC - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/
- MISC - https://about.gitlab.com/2019/02/05/critical-security-release-gitlab-11-dot-7-dot-4-released/
- MISC - https://gitlab.com/gitlab-org/gitlab-ce/issues/57112

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-6797 suppress

An information disclosure issue was discovered in GitLab Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. The GitHub token used in CI/CD for External Repos was being leaked to project maintainers in the UI.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- MISC - https://about.gitlab.com/2019/01/31/security-release-gitlab-11-dot-7-dot-3-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.5.8
- ...

CVE-2019-9170 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control.

CWE-639 Authorization Bypass Through User-Controlled Key

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/51971
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9171 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 1 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: LOW (3.7)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54635
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9172 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 2 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.9)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54795
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9174 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows SSRF.

CWE-918 Server-Side Request Forgery (SSRF)

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (10.0)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/55468
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9175 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 3 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/52524
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9176 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows CSRF.

CWE-352 Cross-Site Request Forgery (CSRF)

CVSSv2:
- Base Score: MEDIUM (5.8)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/55664
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9178 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 4 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54803
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9179 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure (issue 5 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: LOW (3.7)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54783
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9217 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. Its User Interface has a Misrepresentation of Critical Information.

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9218 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 1 of 5).

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9219 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 2 of 5).

CWE-639 Authorization Bypass Through User-Controlled Key

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: LOW (3.7)
- Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54159
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9220 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Uncontrolled Resource Consumption.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/55653
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9221 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 3 of 5).

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: LOW (2.1)
- Vector: /AV:L/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.5)
- Vector: CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:

- MISC - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9222 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.

CWE-732 Incorrect Permission Assignment for Critical Resource, CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CVSSv2:
- Base Score: MEDIUM (5.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:P

CVSSv3:
- Base Score: HIGH (8.1)
- Vector: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/56348
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9223 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It allows Information Exposure.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/50334
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9224 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 4 of 5).

CWE-862 Missing Authorization

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54789
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9225 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Incorrect Access Control (issue 5 of 5).

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.3)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- CONFIRM - https://gitlab.com/gitlab-org/gitlab-ce/issues/54680
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2019-9485 suppress

An issue was discovered in GitLab Community and Enterprise Edition before 11.6.10, 11.7.x before 11.7.6, and 11.8.x before 11.8.1. It has Insecure Permissions.

NVD-CWE-noinfo

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- MISC - https://about.gitlab.com/2019/03/04/security-release-gitlab-11-dot-8-dot-1-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 11.6.10
- ...

CVE-2020-10081 suppress

GitLab before 12.8.2 has Incorrect Access Control. It was internally discovered that the LFS import process could potentially be used to incorrectly access LFS objects not owned by the user.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (4.0)

- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/index.html
- MISC - https://about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.8.1
- ...

CVE-2020-10087 suppress

GitLab before 12.8.2 allows Information Disclosure. Badge images were not being proxied, causing mixed content warnings as well as leaking the IP address of the user.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/index.html
- MISC - https://about.gitlab.com/releases/2020/03/04/gitlab-12-dot-8-dot-2-released/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (including) 12.8.1
- ...

CVE-2020-10954 suppress

GitLab through 12.9 is affected by a potential DoS in repository archive download.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://about.gitlab.com/releases/2020/03/26/security-release-12-dot-9-dot-1-released/
- MISC - https://about.gitlab.com/releases/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (including) 12.9
- ...

CVE-2020-11505 suppress

An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling.

CWE-200 Information Exposure

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/releases/2020/04/14/critical-security-release-gitlab-12-dot-9-dot-3-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.7.9
- ...

CVE-2020-13271 suppress

A Stored Cross-Site Scripting vulnerability allowed the execution of arbitrary Javascript code in the blobs API in all previous GitLab CE/EE versions through 13.0.1

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13271.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/200094
- MISC - https://hackerone.com/reports/672150

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.9.8
- ...

CVE-2020-13274 suppress

A security issue allowed achieving Denial of Service attacks through memory exhaustion by uploading malicious artifacts in all previous GitLab versions through 13.0.1

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13274.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/14195

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.9.8
- ...

CVE-2020-13276 suppress

User is allowed to set an email as a notification email even without verifying the new email in all previous GitLab CE/EE versions through 13.0.1

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13276.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/25994
- MISC - https://hackerone.com/reports/471907

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 12.9.8
- ...

CVE-2020-13280 suppress

For GitLab before 13.0.12, 13.1.6, 13.2.3 a memory exhaustion flaw exists due to excessive logging of an invite email error message.

CWE-400 Uncontrolled Resource Consumption ('Resource Exhaustion')

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13280.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/28291

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:enterprise:*:*:* versions up to (excluding) 13.0.12
- ...

CVE-2020-13296 suppress

An issue has been discovered in GitLab affecting versions >=10.7 <13.0.14, >=13.1.0 <13.1.8, >=13.2.0 <13.2.6. Improper Access Control for Deploy Tokens

CWE-862 Missing Authorization

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13296.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/235996
- MISC - https://hackerone.com/reports/957459

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (including) 10.7
- ...

CVE-2020-13297 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. When 2 factor authentication was enabled for groups, a malicious user could bypass that restriction by sending a specific query to the API endpoint.

CWE-287 Improper Authentication

CVSSv2:
- Base Score: MEDIUM (4.9)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13297.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/32215
- MISC - https://hackerone.com/reports/691592

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13298 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Conan package upload functionality was not properly validating the supplied parameters, which resulted in the limited files disclosure.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (5.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13298.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/228841
- MISC - https://hackerone.com/reports/923027

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13301 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a stored XSS on the standalone vulnerability page.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13301.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/219378
- MISC - https://hackerone.com/reports/882988

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13302 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Under certain conditions GitLab was not properly revoking user sessions and allowed a malicious user to access a user account with an old password.

CWE-613 Insufficient Session Expiration

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.2)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13302.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/25195
- MISC - https://hackerone.com/reports/437194

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13304 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. Same 2 factor Authentication secret code was generated which resulted an attacker to maintain access under certain conditions.

CWE-287 Improper Authentication

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (7.2)
- Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13304.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/27686
- MISC - https://hackerone.com/reports/511260

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13305 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was not invalidating project invitation link upon removing a user from a project.

CWE-613 Insufficient Session Expiration

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13305.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/26801
- MISC - https://hackerone.com/reports/492621

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13306 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab Webhook feature could be abused to perform denial of service attacks due to the lack of rate limitation.

CWE-770 Allocation of Resources Without Limits or Throttling

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13306.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/223681
- MISC - https://hackerone.com/reports/904134

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13309 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. GitLab was vulnerable to a blind SSRF attack through the repository mirroring feature.

CWE-918 Server-Side Request Forgery (SSRF)

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13309.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/215879
- MISC - https://hackerone.com/reports/860196

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13310 suppress

A vulnerability was discovered in GitLab runner versions before 13.1.3, 13.2.3 and 13.3.1. It was possible to make the gitlab-runner process crash by sending malformed queries, resulting in a denial of service.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13310.json
- MISC - https://gitlab.com/gitlab-org/gitlab-runner/-/issues/25857
- MISC - https://gitlab.com/gitlab-org/gitlab-runner/-/issues/26819

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.3
- ...

CVE-2020-13315 suppress

A vulnerability was discovered in GitLab versions before 13.1.10, 13.2.8 and 13.3.4. The profile activity page was not restricting the amount of results one could request, potentially resulting in a denial of service.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13315.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/25825
- MISC - https://hackerone.com/reports/463010

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 13.1.10
- ...

CVE-2020-13319 suppress

An issue has been discovered in GitLab affecting versions prior to 13.1.2, 13.0.8 and 12.10.13. Missing permission check for adding time spent on an issue.

CWE-862 Missing Authorization

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13319.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/201806
- MISC - https://hackerone.com/reports/755188

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 12.10.13
- ...

CVE-2020-13320 suppress

An issue has been discovered in GitLab before version 12.10.13 that allowed a project member with limited permissions to view the project security dashboard.

CWE-863 Incorrect Authorization

CVSSv2:
- Base Score: MEDIUM (4.0)
- Vector: /AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13320.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/215044

Vulnerable Software & Versions:

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 12.10.13

CVE-2020-13321 suppress

A vulnerability was discovered in GitLab versions prior to 13.1. Username format restrictions could be bypassed allowing for html tags to be added.

NVD-CWE-noinfo

CVSSv2:
- Base Score: MEDIUM (6.5)
- Vector: /AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: HIGH (8.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13321.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/25751

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 12.10.13
- ...

CVE-2020-13329 suppress

An issue has been discovered in GitLab affecting versions from 12.6.2 prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the blob view feature.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13329.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/208685

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 12.6.2
- ...

CVE-2020-13330 suppress

An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS in import the Bitbucket project feature.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)

- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13330.json
- MISC - https://gitlab.com/gitlab-org/gitlab/issues/30017

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (including) 11.2.0
- ...

CVE-2020-13331 suppress

An issue has been discovered in GitLab affecting versions prior to 12.10.13. GitLab was vulnerable to a stored XSS by in the Wiki pasges.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (5.4)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13331.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/219010

Vulnerable Software & Versions:

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:*:*:*:* versions up to (excluding) 12.10.13

CVE-2020-13339 suppress

An issue has been discovered in GitLab affecting all versions before 13.2.10, 13.3.7 and 13.4.2: XSS in SVG File Preview. Overall impact is limited due to the current user only being impacted.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (6.0)
- Vector: /AV:N/AC:M/Au:S/C:P/I:P/A:P

CVSSv3:
- Base Score: MEDIUM (6.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:L

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13339.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/118477
- MISC - https://hackerone.com/reports/758653

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 13.2.10
- ...

CVE-2020-13340 suppress

An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2: Stored XSS in CI Job Log

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: LOW (3.5)
- Vector: /AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSSv3:
- Base Score: HIGH (8.7)
- Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:N

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13340.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/233473
- MISC - https://hackerone.com/reports/950190

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 13.2.10
- ...

CVE-2020-13350 suppress

CSRF in runner administration page in all versions of GitLab CE/EE allows an attacker who's able to target GitLab instance administrators to pause/resume runners. Affected versions are >=13.5.0, <13.5.2,>=13.4.0, <13.4.5,<13.3.9.

CWE-352 Cross-Site Request Forgery (CSRF)

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:N/A:P

CVSSv3:
- Base Score: MEDIUM (4.3)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L

References:
- CONFIRM - https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13350.json
- MISC - https://gitlab.com/gitlab-org/gitlab/-/issues/24416
- MISC - https://hackerone.com/reports/415238

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 13.3.9
- ...

CVE-2020-7968 suppress

GitLab EE 8.0 through 12.7.2 has Incorrect Access Control.

CWE-287 Improper Authentication

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:P/I:N/A:N

CVSSv3:
- Base Score: HIGH (7.5)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

References:
- CONFIRM - https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.5.9
- ...

CVE-2020-7973 suppress

GitLab through 12.7.2 allows XSS.

CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

CVSSv2:
- Base Score: MEDIUM (4.3)
- Vector: /AV:N/AC:M/Au:N/C:N/I:P/A:N

CVSSv3:
- Base Score: MEDIUM (6.1)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

References:
- CONFIRM - https://about.gitlab.com/releases/2020/01/30/security-release-gitlab-12-7-4-released/
- MISC - https://about.gitlab.com/blog/categories/releases/
- MISC - https://gitlab.com/gitlab-org/security/gitlab/issues/14

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:gitlab:gitlab:*:*:*:*:community:*:*:* versions up to (excluding) 12.5.9
- ...

modernc.org/file:1.0.0

File Path: /Users/akhode/v4/dss/go.mod:modernc.org/file/1.0.0

Evidence

Identifiers

- pkg:golang/modernc.org/file@1.0.0 (*Confidence*:Highest)
- cpe:2.3:a:file_project:file:1.0.0:*:*:*:*:*:*:* (*Confidence*:High) suppress

Published Vulnerabilities

CVE-2014-8117 suppress

softmagic.c in file before 5.21 does not properly limit recursion, which allows remote attackers to cause a denial of service (CPU consumption or crash) via unspecified vectors.

CWE-399 Resource Management Errors

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- BID - 71692
- CONFIRM - http://advisories.mageia.org/MGASA-2015-0040.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
- CONFIRM - https://github.com/file/file/blob/00cef282a902a4a6709bbbbb933ee397768caa38/ChangeLog
- CONFIRM - https://github.com/file/file/commit/6f737ddfadb596d7d4a993f7ed2141ffd664a81c
- FREEBSD - FreeBSD-SA-14:28
- MLIST - [oss-security] 20141216 file(1): multiple denial of service issues (resource consumption), CVE-2014-8116 and CVE-2014-8117
- REDHAT - RHSA-2016:0760
- SECTRACK - 1031344
- SECUNIA - 61944
- SECUNIA - 62081
- UBUNTU - USN-2494-1
- UBUNTU - USN-2535-1

Vulnerable Software & Versions:

- cpe:2.3:a:file_project:file:*:*:*:*:*:*:*:* versions up to (including) 5.20

CVE-2014-9652 suppress

The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.

CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer

CVSSv2:
- Base Score: MEDIUM (5.0)
- Vector: /AV:N/AC:L/Au:N/C:N/I:N/A:P

References:
- APPLE - APPLE-SA-2015-09-30-3
- BID - 72505
- CONFIRM - http://bugs.gw.com/view.php?id=398
- CONFIRM - http://php.net/ChangeLog-5.php
- CONFIRM - http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
- CONFIRM - https://bugs.php.net/bug.php?id=68735
- CONFIRM - https://bugs.php.net/patch-display.php?bug=68735&patch=bug68735.patch&revision=1420309079
- CONFIRM - https://github.com/file/file/commit/59e63838913eee47f5c120a6c53d4565af638158
- CONFIRM - https://support.apple.com/HT205267
- GENTOO - GLSA-201701-42
- HP - HPSBMU03380
- HP - HPSBMU03409
- MLIST - [oss-security] 20150205 Re: CVE Request: PHP/file: out-of-bounds memory access in softmagic
- REDHAT - RHSA-2015:1053
- REDHAT - RHSA-2015:1066
- REDHAT - RHSA-2015:1135
- SUSE - SUSE-SU-2015:0424
- SUSE - SUSE-SU-2015:0436
- SUSE - openSUSE-SU-2015:0440

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:file_project:file:*:*:*:*:*:*:*:* versions up to (including) 5.20
- ...

CVE-2014-9653 suppress

readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.

CWE-20 Improper Input Validation

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

References:
- BID - 72516
- CONFIRM - http://bugs.gw.com/view.php?id=409
- CONFIRM - http://php.net/ChangeLog-5.php
- CONFIRM - http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html

- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
- CONFIRM - http://www.oracle.com/technetwork/topics/security/linuxbulletinoct2015-2719645.html
- CONFIRM - https://github.com/file/file/commit/445c8fb0ebff85195be94cd9f7e1df89cade5c7f
- DEBIAN - DSA-3196
- GENTOO - GLSA-201701-42
- HP - HPSBMU03380
- HP - HPSBMU03409
- MLIST - [file] 20141216 [PATCH] readelf.c: better checks for values returned by pread
- MLIST - [oss-security] 20150205 Re: CVE Request: PHP/file: out-of-bounds memory access in softmagic
- REDHAT - RHSA-2016:0760
- UBUNTU - USN-3686-1

Vulnerable Software & Versions: (show all)

- cpe:2.3:a:file_project:file:*:*:*:*:*:*:*:* versions up to (including) 5.21
- ...

CVE-2019-18218 suppress

cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write).

CWE-787 Out-of-bounds Write

CVSSv2:
- Base Score: HIGH (7.5)
- Vector: /AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSSv3:
- Base Score: CRITICAL (9.8)
- Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

References:
- CONFIRM - https://security.netapp.com/advisory/ntap-20200115-0001/
- DEBIAN - DSA-4550
- FEDORA - FEDORA-2019-18036b898e
- FEDORA - FEDORA-2019-554c3c691f
- FEDORA - FEDORA-2019-97dcb2762a
- GENTOO - GLSA-202003-24
- MISC - https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=16780
- MISC - https://github.com/file/file/commit/46a8443f76cec4b41ec736eca396984c74664f84
- MLIST - [debian-lts-announce] 20191023 [SECURITY] [DLA 1969-1] file security update
- SUSE - openSUSE-SU-2020:0677
- UBUNTU - USN-4172-1
- UBUNTU - USN-4172-2

Vulnerable Software & Versions:

- cpe:2.3:a:file_project:file:*:*:*:*:*:*:*:* versions up to (including) 5.37

This report contains data retrieved from the National Vulnerability Database.
This report may contain data retrieved from the NPM Public Advisories.
This report may contain data retrieved from RetireJS.
This report may contain data retrieved from the Sonatype OSS Index.