CVE-2019-1002100
Security Release Post Mortem

PUBLIC

Authors: cjcullen@google.com, liggitt@google.com, xuchao@google.com

Status: published
Last updated: 2019-03-05

Impact

- A specifically crafted patch request of type json-patch can make the apiserver panic, consume excessive memory, or consume excessive CPU, causing a potential Denial of Service vulnerability.

See #74534 for details of CVE-2019-1002100.

Timeline

(All times are in PT)

2019-01-15 11:45 AM Reported privately to Kubernetes Product Security Team (PST) by Carl Henrik Lunde

2019-01-15 12:00 PM Report acknowledged by PST (bphilips)

2019-01-15 4:30PM Reproduction of reported issues (xuchao)

2019-01-17 First set of fixes to json-patch opened for review:
https://github.com/evanphx/json-patch/pull/70
https://github.com/evanphx/json-patch/pull/71
https://github.com/evanphx/json-patch/pull/72

2019-01-28 First set of fixes merged to evan-phx/json-patch

2019-01-28 PR open to pull first set of fixes into Kubernetes:
https://github.com/kubernetes/kubernetes/pull/73443

2019-01-31 Additional bugs/DoS vectors discovered (xuchao, liggitt).

2019-02-01 2nd set of fixes to json-patch opened for review:
https://github.com/evanphx/json-patch/pull/74
https://github.com/evanphx/json-patch/pull/73

2019-02-04 PRs start to be sent to pull 2nd set of fixes into Kubernetes:
https://github.com/kubernetes/kubernetes/pull/73443
https://github.com/kubernetes/kubernetes/pull/73805
https://github.com/kubernetes/kubernetes/pull/74000

2019-02-13 PRs to kubernetes/kubernetes master merged

2019-02-13 Cherrypick PRs open:
1.11 - https://github.com/kubernetes/kubernetes/pull/74106
1.12 - https://github.com/kubernetes/kubernetes/pull/74104

1.13 - https://github.com/kubernetes/kubernetes/pull/74102

2019-02-21	Cherrypick PRs merged
2019-02-25 6:00PM	kubernetes-distributors-announce email sent
2019-02-26 6:20PM	v1.12.6 release announced
2019-02-28 9:40AM	v1.13.4 release announced
2019-03-01 8:30AM	v1.11.8 release announced
2019-03-01 9:00AM	Security announcement published, details added to CVE issue

Root Causes and Trigger

- Error conditions were not checked when apiserver handled json-patch requests.
- Use of memory was unbounded when apiserver handled json-patch requests.

Lessons Learned

What worked

- Initial report was thorough.
- Fix team assembled and began investigating quickly.

What can go better

- Distributors were surprised by the small amount of time between distributors-announce and public announcement for a medium severity issue.
- Long lag between 1.11.8 artifacts being available and full release process finishing.

Where we got lucky

- Vulnerability was reported privately.
- Fixes were handled publicly without issue.
- We caught and fixed additional DoS issues before announcing the issues that were reported.

Where we got unlucky

- Part of vulnerability was in another repo/organization, which caused some delays.

Followup

Action Item	Issue, PR, or owner
Fix our use of json-patch	#74534 (fixed)