Bug 1978621 (CVE-2021-3636) - CVE-2021-3636 openshift: Injected service-ca.crt incorrectly contains additional internal CAs

Keywords: Security ×

Status: CLOSED ERRATA
Alias: CVE-2021-3636
Product: Security Response
Component: vulnerability
Version: unspecified
Hardware: All
OS: Linux
Priority: medium
Severity: medium
Target Milestone: ---
Assignee: Red Hat Product Security
QA Contact: ~~liyao~~
Docs Contact:
URL:
Whiteboard:
Depends On: 1979042 1981655 1981658 1981659 1981660
Blocks: 1978624 1978822
TreeView+ depends on / blocked

Reported: 2021-07-02 10:29 UTC by Przemyslaw Roguski
Modified: 2021-11-03 20:53 UTC (History)
CC List: 22 users (show)
Fixed In Version: openshift 4.8
Doc Type: If docs needed, set a value
Doc Text: It was found in OpenShift, before version 4.8, that the generated certificate for the in-cluster Service CA, incorrectly included additional certificates. The Service CA is automatically mounted into all pods, allowing them to safely connect to trusted in-cluster services that present certificates signed by the trusted Service CA. The incorrect inclusion of additional CAs in this certificate would allow an attacker that compromises any of the additional CAs to masquerade as a trusted in-cluster service.
Clone Of:
Environment:
Last Closed: 2021-07-28 01:08:01 UTC

Attachments	(Terms of Use)
Add an attachment (proposed patch, testcase, etc.)	

Links

System	ID	Private	Priority	Status	Summary	Last Updated
Red Hat Product Errata	RHSA-2021:2437	0	None	None	None	2021-07-27 22:07:42 UTC

Przemyslaw Roguski 2021-07-02 10:29:30 UTC — Description

```
The openshift-service-ca service contains unexpected CAs.
In OpenShift 4.8 the service-ca.crt file only contains the self-signed certificate of the openshift-service-serving-signer CA certificate.
In older versions of OpenShift there were more, additional CAs:
- OU = openshift, CN = kube-apiserver-lb-signer
- OU = openshift, CN = kube-apiserver-localhost-signer
- OU = openshift, CN = kube-apiserver-service-network-signer
- CN = openshift-kube-apiserver-operator_localhost-recovery-serving-signer
- CN = ingress-operator
- CN = *.apps.cluster.example.com
- CN = openshift-service-serving-signer


This means that an attacker who owns the ingress CA can impersonate as any in-cluster service-ca signed process.
The issue impacts Confidentiality and Integrity of the OCP cluster.

OCP 4.8 is not impacted by this vulnerability.
```

Sam Fowler 2021-07-13 06:00:41 UTC — Comment 5

```
Fix:

https://github.com/openshift/kubernetes/pull/714
```

Sam Fowler 2021-07-13 06:08:00 UTC — Comment 6

```
In Kubernetes 1.21, which OpenShift 4.8 is based on, the method in which service accounts are mounted in pods changed, to now use projected volumes:

https://kubernetes.io/docs/reference/access-authn-authz/service-accounts-admin/#bound-service-account-token-volume

OpenShift rewrote the way service-ca.crt is injected into pods in 4.8, and now no longer includes the incorrect additional CAs.
```

Sam Fowler 2021-07-13 06:13:48 UTC — Comment 7

```
Below is a comparison of podspecs using the old and new methods of mounting service accounts into pods. In both versions, the injected Service CA will end up in
the same filepath, /var/run/secrets/kubernetes.io/serviceaccount/service-ca.crt.

4.7:
---
spec:
  containers:
    ...
    volumeMounts:
    - mountPath: /tmp
      name: tmp
    - mountPath: /var/run/secrets/kubernetes.io/serviceaccount
      name: default-token-5rk4g
      readOnly: true
        ...
  volumes:
  - emptyDir: {}
    name: tmp
  - name: default-token-5rk4g
    secret:
      defaultMode: 420
      secretName: default-token-5rk4g

4.8
---
spec:
  containers:
    ...
    volumeMounts:
    - mountPath: /tmp
      name: tmp
```

```
    - mountPath: /var/run/secrets/kubernetes.io/serviceaccount
      name: kube-api-access-jgdq2
      readOnly: true
  volumes:
  - emptyDir: {}
    name: tmp
  - name: kube-api-access-jgdq2
    projected:
      defaultMode: 420
        ...
      - configMap:
          items:
          - key: service-ca.crt
            path: service-ca.crt
          name: openshift-service-ca.crt
```

Sam Fowler 2021-07-13 06:16:01 UTC Comment 8

In fixed versions of OpenShift, servica-ca.crt will contain only a single certificate, for the openshift-service-signer-server. Vulnerable versions will include multiple internal CAs. This can be checked with a command like below:

```
$ openssl crl2pkcs7 -nocrl --certfile service-ca.crt  | openssl pkcs7 -print_certs --text -noout | grep 'CN='
        Issuer: CN=ingress-operator@1626066148
        Subject: CN=ingress-operator@1626066148
        Issuer: CN=openshift-service-serving-signer@1626066048
        Subject: CN=openshift-service-serving-signer@1626066048
        ...
```

errata-xmlrpc 2021-07-27 22:07:44 UTC Comment 11

This issue has been addressed in the following products:

  Red Hat OpenShift Container Platform 4.8

Via RHSA-2021:2437 https://access.redhat.com/errata/RHSA-2021:2437

Product Security DevOps Team 2021-07-28 01:08:01 UTC Comment 12

This bug is now closed. Further updates for individual products will be reflected on the CVE page(s):

https://access.redhat.com/security/cve/cve-2021-3636

Richard Theis 2021-09-09 13:12:11 UTC Comment 13

Are other OpenShift version 4 releases impacted by this CVE? Based on https://access.redhat.com/security/cve/cve-2021-3636, it sounds like they are with the only resolution requiring version 4.8. Are there any plans to fix previous version?

~~Rachel A~~ 2021-10-22 14:15:58 UTC Comment 14

https://access.redhat.com/security/cve/CVE-2021-3636, only documents the fix at 4.8 but that releases before 4.8 are affected, can anyone tell me whether CVE-2021-3636 will be fixed in OpenShift 4.7 and 4.6?

Or is this a similar case to ~~https://bugzilla.redhat.com/show_bug.cgi?id=1963232#c25~~ (CVE-2021-33194) where this vulnerability won't be addressed in OpenShift (OCP) 4.7 and 4.6 as both these releases are already in the maintenance support phase?

Sam Fowler 2021-10-24 23:44:29 UTC Comment 15

(In reply to Rachel A from comment #14)
> https://access.redhat.com/security/cve/CVE-2021-3636, only documents the fix
> at 4.8 but that releases before 4.8 are affected, can anyone tell me whether
> CVE-2021-3636 will be fixed in OpenShift 4.7 and 4.6?

OpenShift 4.8.2 is the first released version of OpenShift 4 that has been fixed. Earlier released versions of OpenShift 4 are affected.

> Or is this a similar case to
> ~~https://bugzilla.redhat.com/show_bug.cgi?id=1963232#c25~~ (CVE-2021-33194)
> where this vulnerability won't be addressed in OpenShift (OCP) 4.7 and 4.6
> as both these releases are already in the maintenance support phase?

This CVE is also rated Moderate, like CVE-2021-33194. Even in Full Support phase, only Important and Critical rated vulnerabilities are covered under our support policy:

https://access.redhat.com/support/policy/updates/openshift

Richard Theis 2021-10-29 13:02:58 UTC Comment 16

Does the support policy prevent such CVEs from being fixed? We are really looking for an answer as to whether we may get a fix or we will never get a fix.

Sam Fowler 2021-11-02 03:29:23 UTC Comment 17

(In reply to Richard Theis from comment #16)
> Does the support policy prevent such CVEs from being fixed? We are really
> looking for an answer as to whether we may get a fix or we will never get a
> fix.

No, it does not prevent them from being fixed. Fixes for Moderate and Low CVEs can be requested by raising a support ticket.

Richard Theis 2021-11-03 20:53:46 UTC Comment 18

Thank you. I've opened a support case.