49

CVE-2020-8286: Inferior OCSP verification

Share:

TIMELINE

ospoco submitted a report to curl. Dec 1st (2 ye

cURL (in /lib/vtls/openssl.c) does not check that the certificate serial number in the stapled OCSP response matches the serial number of the certificate it is tryin validate (the peer certificate). This results in a passed validity challenge even when connecting to a site that has had its certificate revoked.
An example program showing the vulnerability and a suggested patch are included.

EXAMPLE:

1. Identify a site with a revoked certificate. (https://revoked.grc.com)
2. Obtain a valid OCSP response for a site signed by the same issuer as the revoked site. (https://www.grc.com). See https://akshayranganath.github.io/OCSP-Validation-With-Openssl/ for a how-to. Use the ocsp option 'respout' to obtain the DER encoded OCSP response. Certificates for www.grc.com are provided. the following command to obtain an OCSP response for the example certificates: $ openssl ocsp -issuer grc_chain.pem -cert grc_cert.pem -text -url http://ocsp.digicert.com -respout grc_ocsp_resp.der
3. See the OCSP behavior without replacing the OCSP response: $ ./curl_ocsp_vuln_test https://revoked.grc.com Curl Error: SSL server certificate status verification FAILED Curl correctly fails.
4. See the OCSP behavior when replacing the OCSP response with that from www.grc.com: $ ./curl_ocsp_vuln_test https://revoked.grc.com --replace_ocsp grc_ocsp_resp.der

Code 28 Bytes   Wrap lines Copy Dow

```
<!DOCTYPE html PUBLIC...

```

The result is that cURL succeeds despite the site having a revoked certificate.

Impact

Certificates are usually revoked because important information, such as the private key, has become known. This could allow an attacker to cause a "validated" connection to an attacker-controlled site by substituting the OCSP response.

1 attachment:
F1100327: curl_ocsp_vuln.zip

bagder curl staff posted a comment. Dec 2nd (2 ye

Thanks! We will investigate.

bagder curl staff posted a comment. Dec 2nd (2 ye

We're just 7 days away from the next release, this might be tough to make a fix for before then. If not, we need to consider that next.

@ospoco, do you happen to have a proposed fix for this issue?

Also, I feel a bit lost in the OCSP (stapling) specs, but do you have any pointer to the details on how a client should verify the serial number as you mention here?

I figure my next step will be to check out the code for this in the openssl tool. I presume it has code for this somewhere.

ospoco posted a comment. Dec 2nd (2 ye

Hi @bagder, I don't know if you were able to download the attached zip file. It has a proposed patch that fixes the issue. If not I can inline it or attach it separately.

The OpenSSL OCSP logic seems correct. The issue is that the information provided in the OCSP response is not used correctly. It only checks for a valid response the same domain, not that the valid response corresponds to the certificate provided.

The core of the patch is this:

Code 596 Bytes   Wrap lines Copy Dow

```
+  // Find the single OCSP response corresponding to the certificate ID
+  ret = OCSP_resp_find_status(br, id, &cert_status, &crl_reason, &rev, &thisupd,
+                              &nextupd);
+  OCSP_CERTID_free(id);
+  if (ret != 1) {
+    failf(data, "Could not find certificate ID in OCSP response");
+    result = CURLE_SSL_INVALIDCERTSTATUS;
+    goto end;
+  }

 +  // Validate the corresponding single OCSP response
 +  if(!OCSP_check_validity(thisupd, nextupd, 300L, -1L)) {
 +    failf(data, "OCSP response has expired");
 +    result = CURLE_SSL_INVALIDCERTSTATUS;
 +    goto end;
 +  }
```

bagder curl staff posted a comment. Dec 2nd (2 ye

Here's @ospoco's patch, just ever so slightly edited to comply with 'checksrc' but with no changes to the logic.

1 attachment:
F1101829: 0001-openssl-make-the-OCSP-verification-verify-the-certif.patch

bagder curl staff updated the severity from High to Medium (6.6). Dec 2nd (2 ye

bagder curl staff posted a comment. Dec 2nd (2 ye

I used the CVSS calculator to update the severity, and I think a 6.6 score seems accurate.

It can also be noted that this is only an attack on libcurl when `CURLOPT_SSL_VERIFYSTATUS` is set by the application, which it isn't by default.

bagder curl staff posted a comment. Dec 2nd (2 ye

While awaiting possible responses from my security team mates, I wrote up a first advisory draft. In an attempt to get this fixed in the 7.74.0 release next week.

@ospoco: let me know how you want to get credited in the advisory.

Inferior OCSP verification

Project curl Security Advisory, December 9th 2020 -
Permalink

VULNERABILITY

libcurl offers "OCSP stapling" via the `CURLOPT_SSL_VERIFYSTATUS` option. When set, libcurl verifies the OCSP response that a server responds with as part of the TLS handshake. It then aborts the TLS negotiation of something is wrong with the response. The same feature can be enabled with `--cert-status` using the curl tool.

As part of the OCSP response verification, a client should verify that the response is indeed set out for the correct certficate. This step was not performed by libcurl when built or told to use OpenSSL as TLS backend.

This flaw would allow an attacker, who perhaps could have breached a TLS server, to provide a fraudulent OCSP response that would appear fine, instead of the real one. Like if the original certificate actually has been revoked.

We are not aware of any exploit of this flaw.

INFO

This flaw has existed in curl since commit
d1cf5d570663d in curl
7.41.0.

The vulnerability is present only if OpenSSL is the designated TLS backend. OCSP stapling is not enabled by default by libcurl, it needs to be explicitly enabled by the application to get used.

OCSP Stapling can be used with any of the TLS based protocols curl supports, including HTTPS, FTPS, SMTPS, POP3S, IMAPS, HTTPS-proxy and more.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2020-XXXX to this issue.

CWE-299: Improper Check for Certificate Revocation

Severity: Medium

AFFECTED VERSIONS

- Affected versions: libcurl 7.41.0 to and including 7.73.0
- Not affected versions: libcurl < 7.41.0 and libcurl >= 7.74.0

Also note that libcurl is used by many applications, and not always advertised as such.

THE SOLUTION

The OCSP response checker function now also verifies that the certificate id is the correct one.

A fix for CVE-2020-XXXX

RECOMMENDATIONS

We suggest you take one of the following actions immediately, in order of preference:

A - Upgrade curl to version 7.74.0

B - Maybe use GnuTLS as a backend ?

C - backport the patch to your curl version

TIMELINE

CREDITS

This issue was initially reported by XXXXX. Patch by XXXXX.

Thanks a lot!

ospoco posted a comment. Dec 2nd (2 ye

@bagder: Could you say:

This issue was identified by an Ospoco customer who wishes to remain anonymous and reported by Ospoco (https://ospo.co).

ospoco posted a comment. Dec 2nd (2 ye

Or better: This issue was identified and patched by an Ospoco customer who wishes to remain anonymous. Reported by Ospoco (https://ospo.co).

dgustafsson curl staff posted a comment. Dec 3rd (2 ye

First off, let me say thanks for the report and for working with the curl security to resolve this. While far from well-versed in OCSP I took a look as well. As far as I ca from reading the (updated) patch, RFC and OpenSSL code this report is a legitimate flaw and the proposed fix correct.

A small nit on the patch: I think the `switch(cert_status)` should have a comment specifying that the three covered cases are the only possible ones. Seeing that statement without a default made me look for dangerous fallthroughs and I doubt I'll be the only reacting like that.

Regarding the advisory:

> It then aborts the TLS negotiation of something is wrong with the response.

s/of/if/

> a client should verify that the response is indeed set out for the correct certficate.

s/certficate/certificate/

> B - Maybe use GnuTLS as a backend ?

This doesn't seem altogether clear. I assume this refers to fixing scripts/programs which may invoke OCSP stapling using the system supplied curl binary. Since th is nothing that makes GnuTLS a better choice than others, I would say "another TLS backend" instead. Fixing this in an app using libcurl requires recompilation the might as well recompile without OCSP stapling enabled and still use OpenSSL?

Reading this code I'm a bit confused about why we don't set up the OCSP callback and instead run `verifystatus` explicitly? While not necessarily wrong, it seems against OpenSSL documentation.
As a follow-up patch I think we should consider adding the revocation time to the `failf` print on revoked certificate, but that's not related to the issue so not her

bagder curl staff updated CVE reference to CVE-2020-8286. Dec 3rd (2 ye

bagder curl staff posted a comment. Dec 3rd (2 ye

I wasn't very happy with the GnuTLS mention, but OCSP stapling is only supported in three backends and the third one is NSS... I'll remove that advice all together instead say "don't rely on OCSP stapling" for B and remove C.

bagder curl staff posted a comment. Dec 3rd (2 ye

On the patch: I think I rather insert a 'default' to equal unknown, just to remove the doubt for readers.

bagder curl staff posted a comment. Dec 3rd (2 ye

Here's the updated patch

1 attachment:
F1102720: 0001-openssl-make-the-OCSP-verification-verify-the-certif.patch

bagder curl staff posted a comment. Dec 3rd (2 ye

Here's the updated advisory.

1 attachment:
F1102721: CVE-2020-8286.md

bagder curl staff changed the status to ○ **Triaged**. Dec 3rd (2 ye

Dec 3rd (2 years ago)
bagder curl staff changed the report title from **Flaw in OCSP validation logic allows "validated" connection to site with revoked certificate** to **CVE-2020-8286: Inferior OCSP verification**.

dgustafsson curl staff posted a comment. Dec 3rd (2 ye

+1 on the updated patch and advisory.

bagder curl staff posted a comment. Dec 3rd (2 ye

I think we can manage get this into the 7.74.0 release as stated in the advisory. I will alert the distros about it tomorrow morning my time. Just in case anyone read this wants to jump in and do some edits before that happens.

curl rewarded ospoco with a **$900** bounty. Dec 3rd (2 ye

The curl security team has decided to reward hacker @ospoco with the amount of 900 USD for finding, reporting and fixing this issue. Many thanks for your great w

ghedo joined this report as a participant. Dec 3rd (2 ye bagder curl staff requested to disclose this report. Dec 9th (2 ye

ospoco agreed to disclose this report. Dec 9th (2 ye

This report has been disclosed. Dec 9th (2 ye