Message-ID: <20221101170833.GA10470@openwall.com>
Date: Tue, 1 Nov 2022 18:08:34 +0100
From: Solar Designer <solar@...nwall.com>
To: oss-security@...ts.openwall.com
Subject: OpenSSL X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602), X.509 Email Address Variable Length Buffer Overflow (CVE-2022-3786)

I don't know whether the OpenSSL project would be posting this to
oss-security themselves (they really should have), but with publications
elsewhere out for an hour or so I felt it's best if I forward in here.

There's also a blog post with a FAQ:

https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

----- Forwarded message from OpenSSL <openssl@...nssl.org> -----

Date: Tue, 1 Nov 2022 16:16:40 +0000
From: OpenSSL <openssl@...nssl.org>
To: openssl-project@...nssl.org,
 OpenSSL User Support ML <openssl-users@...nssl.org>,
 OpenSSL Announce ML <openssl-announce@...nssl.org>
Subject: OpenSSL Security Advisory

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

OpenSSL Security Advisory [01 November 2022]
==========

X.509 Email Address 4-byte Buffer Overflow (CVE-2022-3602)
==========

Severity: High

A buffer overrun can be triggered in X.509 certificate verification,
specifically in name constraint checking. Note that this occurs
after certificate chain signature verification and requires either a
CA to have signed the malicious certificate or for the application to
continue certificate verification despite failure to construct a path
to a trusted issuer. An attacker can craft a malicious email address
to overflow four attacker-controlled bytes on the stack. This buffer
overflow could result in a crash (causing a denial of service) or
potentially remote code execution.

Many platforms implement stack overflow protections which would mitigate
against the risk of remote code execution. The risk may be further
mitigated based on stack layout for any given platform/compiler.

Pre-announcements of CVE-2022-3602 described this issue as CRITICAL.
Further analysis based on some of the mitigating factors described above
have led this to be downgraded to HIGH. Users are still encouraged to
upgrade to a new version as soon as possible.

In a TLS client, this can be triggered by connecting to a malicious
server. In a TLS server, this can be triggered if the server requests
client authentication and a malicious client connects.

OpenSSL versions 3.0.0 to 3.0.6 are vulnerable to this issue.

OpenSSL 3.0 users should upgrade to OpenSSL 3.0.7.

OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

This issue was reported to OpenSSL on 17th October 2022 by Polar Bear.

```
The fixes were developed by Dr Paul Dale.

We are not aware of any working exploit that could lead to code execution,
and we have no evidence of this issue being exploited as of the time of
release of this advisory (November 1st 2022).

X.509 Email Address Variable Length Buffer Overflow (CVE-2022-3786)
==========================================================================

Severity: High

A buffer overrun can be triggered in X.509 certificate verification,
specifically in name constraint checking. Note that this occurs after
certificate chain signature verification and requires either a CA to
have signed a malicious certificate or for an application to continue
certificate verification despite failure to construct a path to a trusted
issuer. An attacker can craft a malicious email address in a certificate
to overflow an arbitrary number of bytes containing the `.' character
(decimal 46) on the stack. This buffer overflow could result in a crash
(causing a denial of service).

In a TLS client, this can be triggered by connecting to a malicious
server. In a TLS server, this can be triggered if the server requests
client authentication and a malicious client connects.

OpenSSL versions 3.0.0 to 3.0.6 are vulnerable to this issue.

OpenSSL 3.0 users should upgrade to OpenSSL 3.0.7.

OpenSSL 1.1.1 and 1.0.2 are not affected by this issue.

This issue was discovered on 18th October 2022 by Viktor Dukhovni while
researching CVE-2022-3602. The fixes were developed by Dr Paul Dale.

We have no evidence of this issue being exploited as of the time of
release of this advisory (November 1st 2022).

References
==========

URL for this Security Advisory:
https://www.openssl.org/news/secadv/20221101.txt

Note: the online version of the advisory may be updated with additional details
over time.

For details of OpenSSL severity classifications please see:
https://www.openssl.org/policies/secpolicy.html
-----BEGIN PGP SIGNATURE-----

iQJGBAEBCAAwFiEE3HAyZir4heL0fyQ/UnRmohynnm0FAmNhRdsSHHRvbWFzQG9w
ZW5zc2wub3JnAAoJEFJ0ZqIcp55tARIP/R4TFlh4N3wH4enjT74oJowxjmwNIu0q
uRTmmwtMwJOd1Nw0tfydVEtd3qaN/KMcMnnBMzIzvCdzQ202g8SRSzX7zeHZtAEe
idu9qQyQep1ECK7UGybdN+4Ahey30Py6J99okWejCmdHSpxo7+OOtADFdraqrV5A
5vwyojD1Iv95Z0/RqYxMmMBEoJZitsGxeraw1IxBJCqw6sL2WwDelGb9NZwKFee1
BrfeF+dwaXlAZ97Hsaai6ssDf8VOoTNbCDsrsnbo4MAbFAc6ZraynMcWMm9kwF96
y+pO+0P9etzWeHkP+qHAeCCHZqU76Rexr58XtuWQpTdmbPbmLpnwr7wgwBAZxHA0
RkhpR244vPLYrF3cIssNxEstHCi2NFX0cMtOnbY84lJfmnxgHTJqH/7LvUmHibC6
FBNM9CCSezZgEiSvERB0R/auHZnpODj9riCyWWq82sXTkk3XrqkdnN3mAjgVpnDK
3Cacx9vJxpUDl2U4ObEVCE1I1qHKomAcKVAErAMmLLsdkbzoK9dUquG2VhFaJYJW
3TtqDMhQM0fqRgRu750P42w6dm1glH/UIK41viB0eVwbBZ0RdaAnI3+Tuk2NXH2o
nZdH5Lx6scgS+l4K+IF2WzO+WCYThG0Sg22hC6NnFbdksoGA/XaXl80Kf5Ec1LJr
QLeTSjQDj6Fc
=8mrQ
-----END PGP SIGNATURE-----

----- End forwarded message -----
```