OpenSSL 3.0.0 to 3.0.6 decodes some punycode email addresses in X.509 certificates improperly

Vulnerability Note VU#794340

Original Release Date: 2022-11-01 | Last Revised: 2024-03-08

Overview

Two buffer overflow vulnerabilities were discovered in OpenSSL versions 3.0.0 through 3.0.6. These vulnerabilities were introduced in version 3.0.0 with the inclusion of support for punycode email address parsing for X.509 certificates. OpenSSL's assessment of the severity of the vulnerabilities has reduced from CRITICAL to HIGH, and OpenSSL 3.0.7 addresses the issues.

ABOUT VULNERABILITY NOTES

CONTACT US ABOUT THIS VULNERABILITY

PROVIDE A VENDOR STATEMENT

Description

Two buffer overflows have been reported in the OpenSSL 3.0.x branch prior to version 3.0.7 that, when exploited, may lead to denial of services or, in some cases, remote code execution in the vulnerable target environment. OpenSSL client and server implementations that use the vulnerable libraries are affected. The server implementation also requires that TLS client authentication is enabled in order to attack, and potentially exploit, a vulnerable target. OpenSSL provides details:

```
* Fixed two buffer overflows in punycode decoding funct

  A buffer overrun can be triggered in X.509 certifica
  specifically in name constraint checking. Note that
  certificate chain signature verification and require
  have signed the malicious certificate or for the app
  certificate verification despite failure to construc
  issuer.

  In a TLS client, this can be triggered by connecting
  server.  In a TLS server, this can be triggered if t
  client authentication and a malicious client connect

  An attacker can craft a malicious email address to c
  an arbitrary number of bytes containing the `.`  cha
  on the stack.  This buffer overflow could result in
  denial of service).
  ([CVE-2022-3786])

  An attacker can craft a malicious email address to c
  attacker-controlled bytes on the stack.  This buffer
  result in a crash (causing a denial of service) or p
  execution depending on stack layout for any given pl
  ([CVE-2022-3602])
```

OpenSSL versions 1.1.1 and 1.0.2 are not affected.

CERT/CC is unaware of any exploitation of this vulnerability at this time.

Impact

Successful exploitation could lead to denial of service or remote execution of arbitrary code in the target environment.

Solution

Any services depending on versions of OpenSSL 3.0.x prior to OpenSSL 3.0.7 should be upgraded to version 3.0.7 or later. Operators may also consider temporarily disabling TLS client authentication until applying an update.

Acknowledgements

Thanks to OpenSSL for coordinating and remediating the vulnerability. Polar Bear is credited as having discovered CVE-2022-3602. Viktor Dukhovni is reported as the source of CVE-2022-3786.

This document was written by Kevin Stephens, Eric Hatleback, Vijay Sarvepalli, and Jeffrey S. Havrilla.

Vendor Information

Filter by status: All

Filter by content: Additional information available

Sort by: Status

Expand all

Adobe	Affected
Barracuda Networks	Affected
Citrix	Affected
Crestron Electronics	Affected
Digi International	Affected
FreeRADIUS	Affected
Fujitsu Europe	Affected
HardenedBSD	Affected
Iconics Inc.	Affected
Illumos	Affected

View all 1554 vendors

References

- https://www.openssl.org/news/secadv/20221101.txt
- https://gist.github.com/FiloSottile/611fc3fa95c3aceebf2580983f76148c
- https://github.com/NCSC-NL/OpenSSL-2022/tree/main/software
- https://www.openssl.org/blog/blog/2022/11/01/email-address-overflows/

Other Information

CVE IDs:	CVE-2022-3602 CVE-2022-3786
API URL:	VINCE JSON | CSAF
Date Public:	2022-11-01
Date First Published:	2022-11-01
Date Last Updated:	2024-03-08 18:27 UTC
Document Revision:	32

Sponsored by CISA.

Carnegie Mellon University
Software Engineering
Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
412-268-5800

Contact SEI

Contact CERT/CC

412-268-5800
cert@cert.org