



Try



[R2] LCE 4.8.2 Fixes Multiple Third-party Library Vulnerabilities

Critical[← View more security advisories](#)

Synopsis

LCE 4.8.1 is possibly impacted by multiple vulnerabilities reported in third-party libraries. Tenable has not investigated each one to determine if it is exploitable or the vulnerable code path can be reached. Instead, Dev has upgraded the impacted libraries as a faster and safer alternative. Due to the number of library upgrades and the potential for any of these issues to impact LCE users, we strongly encourage you to upgrade. In some cases, older versions than 4.8.0 may be impacted by a subset of these issues.

The following vulnerabilities have been resolved with the updated libraries. Note that several of these issues do not have a CVE assigned.

- SQLite ATTACH / DETACH Statement Handling NULL Pointer Dereference DoS
- curl IDNA Puny Code Translation Incorrect Host Resolution Weakness
- curl tool_urlglob.c Globbing Feature Out-of-bounds Access Issues
- curl lib/escape.c curl_easy_unescape() Function URL Unescape Integer Truncation Heap Buffer Overflow
- curl lib/url.c ConnectionExists() Function Connection Reuse Case-insensitive Password Comparison Remote Weakness
- curl lib/parsedate.c parsedate() Function Out-of-bounds Read Issue
- curl lib/cookie.c Shared Cookies Handling Use-after-free Information Disclosure
- curl lib/mprintf.c alloc_addbyter() Function Double-free DoS



Try



Unspecified Issue

- curl lib/base64.c base64_encode() Function Integer Overflow Heap Buffer Overflow
- curl lib/escape.c Multiple Functions String Length Handling Integer Overflow Heap Buffer Overflow
- OpenSSL ssl/t1_lib.c ssl_parse_clienthello_tlsext() Function OCSP Status Request Extension Handling Memory Exhaustion Remote DoS
- OpenSSL Certificate Message Handling Limited Out-of-bounds Read DoS Weakness
- OpenSSL ssl/statem/statem_dtls.c dtls1_preprocess_fragment() Function DTLS Message Handling Memory Exhaustion Remote DoS
- OpenSSL ssl/record/rec_layer_s3.c SSL_peek() Function Empty Record Handling Remote DoS
- OpenSSL ssl/statem/statem_lib.c tls_get_message_header() Function Memory Exhaustion Remote DoS
- OpenSSL crypto/mdc2/mdc2dgst.c MDC2_Update() Function Buffer Overflow Weakness
- OpenSSL ssl/t1_lib.c tls_decrypt_ticket() Function Ticket HMAC Digest Handling Remote DoS
- OpenSSL DTLS Buffered Message Saturation Queue Exhaustion Remote DoS
- OpenSSL DTLS Implementation Record Epoch Sequence Number Handling Remote DoS
- OpenSSL crypto/bn/bn_print.c BN_bn2dec() Function BIGNUM Handling Buffer Overflow DoS
- OpenSSL crypto/ts/ts_lib.c TS_OBJ_print_bio() Function Out-of-bounds Read Issue
- OpenSSL crypto/dsa/dsa_ossl.c DSA Signing Algorithm Constant Time Failure Side-channel Attack Information Disclosure
- OpenSSL Integer Overflow Unspecified Weakness
- Triple Data Encryption Algorithm (3DES) 64-bit Block Size Birthday Attack HTTPS Cookie MitM Disclosure (SWEET32)

Note that the CVSSv2 score associated with this advisory is specific to the cURL / libcurl integration into LCE and assumes a worst-case scenario. These updates are proactive; Tenable has had no reports of exploitation and some of these issues may not impact LCE at all. Please note that Tenable strongly recommends that LCE be installed on a subnet that is not Internet addressable.



Try

[Support Center](#)

Additional References

http://static.tenable.com/prod_docs/upgrade_lce.html#482

<https://www.openssl.org/news/secadv/20160922.txt>

This page contains information regarding security vulnerabilities that may impact Tenable's products. This may include issues specific to our software, or due to the use of third-party libraries within our software. Tenable strongly encourages users to ensure that they upgrade or apply relevant patches in a timely manner.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email advisories@tenable.com

Risk Information

CVE ID: [CVE-2016-2177](#)

[CVE-2016-2178](#)

[CVE-2016-2179](#)

[CVE-2016-2180](#)

[CVE-2016-2181](#)

[CVE-2016-2182](#)

[CVE-2016-2183](#)

[CVE-2016-6302](#)

[CVE-2016-6303](#)

[CVE-2016-6304](#)

[CVE-2016-6305](#)

[CVE-2016-6306](#)

[CVE-2016-6307](#)

[CVE-2016-6308](#)

[CVE-2016-8615](#)

[CVE-2016-8616](#)



Try

[CVE-2016-8621](#)[CVE-2016-8622](#)[CVE-2016-8623](#)[CVE-2016-8624](#)[CVE-2016-8625](#)**Tenable Advisory ID:** TNS-2016-21**Risk Factor:** Critical**CVSSv2 Base / Temporal Score**

10.0 / 7.4

CVSSv2 Vector:

(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)

Affected Products

Log Correlation Engine (LCE) 4.8.1

Disclosure Timeline

2016-12-21 - LCE 4.8.2 released

Advisory Timeline

2016-12-21 - [R1] Initial Release

2017-02-28 - [R2] Adjust CVSS for worst-case scenario (AV:A -> AV:N)

>



Featured products

Tenable One Exposure Management Platform

Tenable Cloud Security (CNAPP)

Tenable Cloud Vulnerability Management

Tenable CIEM

Tenable Vulnerability Management

[Try](#)[Tenable Enclave Security](#)[Tenable Attack Surface Management](#)[Tenable Nessus](#)[Tenable AI Exposure](#)[Tenable OT Security](#)[Tenable Identity Exposure](#)[View all >](#)

Featured solutions

[Active Directory](#)[Building management systems](#)[Cloud security posture management](#)[Compliance](#)[Exposure management](#)[Banks and financial services](#)[Healthcare](#)[Hybrid cloud security](#)[IT/OT](#)[Ransomware](#)[State / Local / Education](#)[US federal](#)[Vulnerability management](#)[Zero trust](#)[View all >](#)

Customer resources

[Resource library](#)



Try



Tenable Research

Documentation

Cybersecurity guide

Why Tenable

Trust

System status

Connections

Blog

Contact us

Careers

Investors

Tenable Ventures

Events

Media

Privacy policy

Do not sell/share my personal information

Legal

508 compliance

© 2026 Tenable®, Inc. All rights reserved

