unify

Security Advisory Report - OBSO-1709-01

curl / libcurl Function TFTP File Name Handling Out-of-bounds Read Issue (CVE-2017-1000100)

Creation Date: 2017-09-21
Last Update: 2017-09-21

Summary

Libcurl vulnerability: TFTP given a URL that contains a very long file name

A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL.

Products that use TFTP transfer via libcurl are affected.

Vulnerability Details

When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length.
This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer.
The sendto() function will then read beyond the end of the heap based buffer.

A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.

We are not aware of any exploit of this flaw.

This bug has been present in curl since TFTP support was added, in September 2005 (commit 56d9624b566).

Affected versions: libcurl 7.15.0 to and including 7.54.1

Not affected versions: libcurl < 7.15.0 and >= 7.55.0

libcurl is used by many applications, but not always advertised as such

A patch for CVE-2017-1000100 is available.The function now returns error if attempting to send a file name that is too long to fit in the TFTP packet.

This flaw also affects the curl command line tool.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2017-1000100 to this issue.

Affected Products

Affected Products
All Unify products deploying and using libcurl:

OpenScape 4000 and 4000 Assistant V7 and V8
OpenScape Branch and SBC V8 and 9
OpenScpae Xpressions V7
OpenScape Business V2
OpenScape Diagnostic Data Collector
OpenScape Contact Center V9
are not affected by this vulnerability.

All other products do not use libcurl and are thus not affected anyhow.

Recommended Actions

Recommendations:

No Unify product is affected, none of them uses TFTP transfer vial libcurl

For other products:

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

A - Upgrade curl and libcurl to version 7.55.0

B - Apply the patch to your version and rebuild

C - Disable TFTP or otherwise restrict TFTP transfers

References

https://curl.haxx.se/docs/adv_20170809B.html

https://curl.haxx.se/CVE-2017-1000100.patch

https://access.redhat.com/security/cve/cve-2017-1000100

https://github.com/curl/curl/commit/358b2b131ad6c095696f20dcfa62b8305263f898

Revision History

first draft 2017-09-08

Released 2017-09-21

Advisory ID: OBSO-1709-01 (a=165), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com

The information provided in this document contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.
Unify, OpenScape, OpenStage and HiPath are registered trademarks of Unify Software and Solutions GmbH & Co. KG.
All other company, brand, product and service names are trademarks or registered trademarks of their respective holders.