CVE-2016-9594

uninitialized random

Related:
Audits
Changelog
curl CVEs
JSON metadata
Vulnerability Disclosure
Vulnerabilities Table

Project curl Security Advisory, December 23 2016
Permalink

VULNERABILITY

libcurl's (new) internal function that returns a good 32-bit random value was implemented poorly and overwrote the pointer instead of writing the value into the buffer the pointer pointed to.

This random value is used to generate nonces for Digest and NTLM authentication, for generating boundary strings in HTTP formposts and more. Having a weak or virtually non-existent random there makes these operations vulnerable.

This function is brand new in 7.52.0 and is the result of an overhaul to make sure libcurl uses strong random as much as possible - provided by the backend TLS crypto libraries when present.

INFO

This mistake managed to slip in because:

1. It was not detected by manual code reviews
2. When libcurl is built debug-enabled (which is often the case when libcurl developers build it), the bug does not trigger.
3. When built without -g, the test suite's "valgrind output parser" wrongly ignored the valgrind output and with libcurl's standard build it is typically built without -g. Thus hiding this problem to most users.

The Common Vulnerabilities and Exposures (CVE) project has assigned the name CVE-2016-9594 to this issue.

CWE-330: Use of Insufficiently Random Values

Severity: High

AFFECTED VERSIONS

This flaw exists in the following libcurl versions.

- Affected versions: libcurl 7.52.0 to and including libcurl 7.52.0
- Not affected versions: libcurl < 7.52.0 and libcurl >= 7.52.1
- Introduced-in: https://github.com/curl/curl/commit/f682156a4fc6c43fb

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

SOLUTION

In version 7.52.1, we fixed the function and we fixed the valgrind parser in the test suite.

- Fixed-in: https://github.com/curl/curl/commit/f81b2277a8e7e9ce880

RECOMMENDATIONS

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

A - Upgrade curl and libcurl to version 7.52.1

B - Apply the patch to 7.52.0 and rebuild

TIMELINE

It was first reported to the curl project on December 21 by Kamil Dudka.

We contacted distros@openwall on December 21.

curl 7.52.1 was released on December 23 2016, coordinated with the publication of this advisory.

CREDITS

- Reported-by: Kamil Dudka
- Patched-by: Kamil Dudka

Thanks a lot!