



CVE-2018-20840

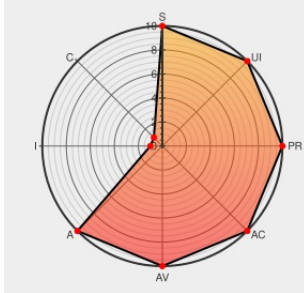
Published on: 05/30/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:35 PM UTC

CVE-2018-20840

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H



Certain versions of [Api C Client](#) from [Google](#) contain the following vulnerability:

An unhandled exception vulnerability exists during Google Sign-In with Google API C++ Client before 2019-04-10. It potentially causes an outage of third-party services that were not designed to recover from exceptions. On the client, ID token handling can cause an unhandled exception because of misinterpretation of an integer as a string,

resulting in denial-of-service and then other users can no longer login/sign-in to the affected third-party service. Once this third-party service uses Google Sign-In with google-api-cpp-client, a malicious user can trigger this client/auth/oauth2_authorization.cc vulnerability by requesting the client to receive the ID token from a Google authentication server.

CVE-2018-20840 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link				
Fixed 'exp' handling in ID token by sungjungk · Pull Request #58 · google/google-api-cpp-client · GitHub	Issue Tracking Patch Third Party Advisory github.com text/html	MISC github.com/google/google-api-cpp-client/pull/58				
Error on 'exp' type handling in ID Token · Issue #57 · google/google-api-cpp-client · GitHub	Exploit Issue Tracking Third Party Advisory github.com text/html	MISC github.com/google/google-api-cpp-client/issues/57				
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.						
There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Api C Client	All	All	All	All
Application	Google	Api C Client	All	All	All	All
Application	Google	Api C Client	All	All	All	All
cpe:2.3:a:google:api_c++_client:*****:						
cpe:2.3:a:google:api_c\+\+_client:*****:						
cpe:2.3:a:google:api_c\+\+_client:*****:						
No vendor comments have been submitted for this CVE						
← Previous ID Next ID →						