



CVE-2019-5617

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2019-5617
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-11-06 19:15:00 UTC
Updated	2021-09-14 12:05:00 UTC
Description	Computing For Good's Basic Laboratory Information System (also known as C4G BLIS) version 3.4 and earlier suffers from

Risk And Classification

Problem Types: CWE-306

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gatech	Computing For Goods Basic Laboratory Information System	All	All	All	All
Application	Gatech	Computing For Goods Basic Laboratory Information System	All	All	All	All

References

Reference	Source
R7-2019-09 CVE-2019-5617, CVE-2019-5643, CVE-2019-5644: C4G BLIS authentication and authorization vulnerabilities (FIXED)	MISC
CVE Program record	CVE.C
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: This vulnerability was first discovered privately and reported internally by C4G BLIS team member Aditi Shah in December 2018. Jacob Robles of Rapid7 rediscovered and reported these issues in March of 2019 per Rapid7's vulnerability disclosure policy (<https://www.rapid7.com/security/disclosure/>).

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)