



CVE-2020-7352

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

Summary

CVE	CVE-2020-7352
State	PUBLIC
Assigner	cve@rapid7.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-06 16:15:00 UTC
Updated	2022-08-05 19:31:00 UTC
Description	The GalaxyClientService component of GOG Galaxy runs with elevated SYSTEM privileges in a Windows environment. Du

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gog	Galaxy	All	All	All	All
Application	Gog	Galaxy	All	All	All	All

References

Reference	Source	Link
GOG Galaxy Client Privilege Escalation Module by jtesta · Pull Request #13444 · rapid7/metasploit-framework · GitHub	MISC	github
Positron Security	MISC	www.p
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

Vendor Comments And Credit

Discovery Credit

LEGACY: This issue was discovered and reported to Rapid7 by Joe Testa via the Metasploit Framework.

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](#)