



CVE-2021-32051

Published on: 05/13/2021 12:00:00 AM UTC

Last Modified on: 05/21/2021 04:13:00 PM UTC

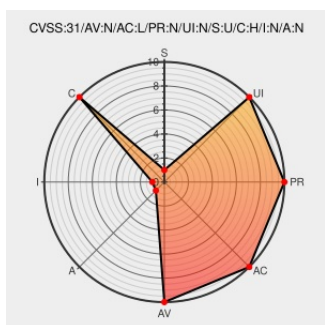
CVE-2021-32051

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Intergraph G!nius](#) from [Hexagon](#) contain the following vulnerability:

Hexagon G!nius Auskunftsportal before 5.0.0.0 allows SQL injection via the GiPWorkflow/Service/DownloadPublicFile id parameter.

CVE-2021-32051 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
Intergraph G!NIUS Hexagon Safety & Infrastructure	www.hexagonsafetyinfrastructure.com/text/html	MISC www.hexagonsafetyinfrastructure.com/products/utilities-and-communications

 MISC packetstormsecurity.com/files/162534/Hexagon-G-nius-Auskunftsportal-SQL

 MISC
gist.githubusercontent.com/mke1985/a21a71098f48829916dfec74eff1e24a/raw/f635b02021-32051

Page 1 of 1

Known Affected Configurations (CPE V2.3)

No vendor comments have been submitted for this CVE

Source	Title	Posted (UTC)
@SecurityNewsbot	CVE-2021-32051 Hexagon GInius Auskunftportal before 5.0.0.0 allows SQL #injection via the GiPWor... seclists.org/fulldisclosure... #FullDisclosure	2021-05-11 17:45:11
@pwnwikiorg	CVE-2021-32051 Hexagon GInius Auskunftportal SQL 注入漏洞 pwnwiki.org/index.php?titl...	2021-05-12 08:59:21
@CVEreport	CVE-2021-32051 : Hexagon GInius Auskunftportal before 5.0.0.0 allows SQL injection via the GiPWorkflow/Service/Dow... twitter.com/i/web/status/1...	2021-05-14 01:04:55
/r/netcve	CVE-2021-32051	2021-05-14 01:41:20

Next ID→

CVE.report and Source URL Uptime Status status.cve.report