



VDB-202981 · CVE-2022-2262

ONLINE HOTEL BOOKING SYSTEM 1.0 ROOM EDIT_ALL_ROOM.PHP ID SQL INJECTION

CVSS Meta Temp Score (?)

4.5

Current Exploit Price (≈) (?)

\$0-\$5k

CTI Interest Score (?)

0.00

A vulnerability has been found in Online Hotel Booking System 1.0 (Hospitality Software) and classified as critical. Affected by this vulnerability is some unknown functionality of the file *edit_all_room.php* of the component *Room Handler*. The manipulation of the argument `id` with the input value `2828%27%20AND%20(SELECT%203766%20FROM%20(SELECT(SLEEP(5)))BmIK)%20AND%20%27YLP1%27=%27YLP1` leads to a sql injection vulnerability. The CWE definition for the vulnerability is CWE-89. The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component. As an impact it is known to affect confidentiality, integrity, and availability.

The weakness was released 06/30/2022. The advisory is shared at github.com. This vulnerability is known as CVE-2022-2262. Technical details and also a public exploit are known. MITRE ATT&CK project uses the attack technique T1505 for this issue.

It is declared as proof-of-concept. It is possible to download the exploit at github.com. By approaching the search of `inurl:edit_all_room.php` it is possible to find vulnerable targets with Google Hacking.

There is no information about possible countermeasures known. It may be suggested to replace the affected object with an alternative product.

Product

Type

- Hospitality Software

Name

- Online Hotel Booking System

CPE 2.3

-

CPE 2.2

- 

CVSSv3

VulDB Meta Base Score: 4.7

VulDB Meta Temp Score: 4.5


VulDB Base Score: 4.7

VulDB Temp Score: 4.3

VulDB Vector: 

VulDB Reliability: 

CNA Base Score: 4.7

CNA Vector (VulDB): 

CVSSv2



VulDB Base Score: 

VulDB Temp Score: 

VulDB Reliability: 

Exploiting

Class: Sql injection

CWE: CWE-89 / CWE-74 / CWE-707

ATT&CK: T1505

Local: No

Remote: Yes

Availability: 

Access: Public

Status: Proof-of-Concept

Download: 

Google Hack: 🔒

EPSS Score: 🔒

EPSS Percentile: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: no mitigation known

Status: 🔍

0-Day Time: 🔒

Timeline

06/30/2022		Advisory disclosed
06/30/2022	+0 days	CVE reserved
06/30/2022	+0 days	VulDB entry created
07/17/2022	+17 days	VulDB last update

Sources

Advisory: github.com

Status: Not defined

CVE: CVE-2022-2262 (🔒)

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 06/30/2022 12:24 PM

Updated: 07/17/2022 08:08 AM

Changes: 06/30/2022 12:24 PM (42), 06/30/2022 12:25 PM (1), 07/17/2022 08:02 AM (2), 07/17/2022 08:08 AM (11)

Complete: 

Submitter: webray.com.cn

Discussion

No comments yet. Languages: en.

Please log in to comment.