



CVE-2017-10001

Published on: 08/08/2017 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:29 PM UTC

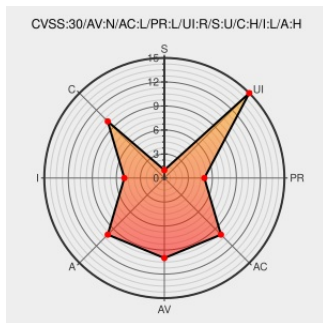
CVE-2017-10001

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Hospitality Symphony](#) from [Oracle](#) contain the following vulnerability:

Vulnerability in the Oracle Hospitality Symphony First Edition component of Oracle Hospitality Applications (subcomponent: Core). The supported version that is affected is 1.7.1. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Symphony First Edition.

Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality Symphony First Edition accessible data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Symphony First Edition accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Hospitality Symphony First Edition. CVSS 3.0 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:H).

CVE-2017-10001 has been assigned by [secalert_us@oracle.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Oracle Corporation - Hospitality Symphony First Edition** version = 1.7.1

CVSS3 Score: **7.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	LOW	HIGH

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

NETWORK

MEDIUM

SINGLE

Confidentiality Impact

Integrity Impact

Availability Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Oracle Hospitality Applications Multiple Flaws Let Remote and Local Users Access and Modify Data and Deny Service - SecurityTracker

Third Party Advisory

VDB Entry

www.securitytracker.com

text/html

SECTrack 1038941

Oracle Critical Patch Update - July 2017

Patch

Vendor Advisory

www.oracle.com

text/html

CONFIRM

www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type

Vendor

Product

Version

Update

Edition

Language

Application

Oracle

Hospitality Symphony

1.7.1

All

All

All

Application

Oracle

Hospitality Symphony

1.7.1

All

All

All

cpe:2.3:a:oracle:hospitality_symphony:1.7.1:*:*:*:first:*:*:

cpe:2.3:a:oracle:hospitality_symphony:1.7.1:*:*:*:first:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →