



CVE-2017-10397

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

Summary

CVE	CVE-2017-10397
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-19 17:29:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	Vulnerability in the Oracle Hospitality Cruise Fleet Management component of Oracle Hospitality Applications (subcomponent of Oracle Hospitality Applications) that allows an attacker to execute arbitrary code on the target system. The vulnerability exists in the <code>com.oracle.hospitality.cruise.fleetmanagement</code> package. The vulnerability is due to a buffer overflow in the <code>com.oracle.hospitality.cruise.fleetmanagement</code> package. An attacker can exploit this vulnerability to execute arbitrary code on the target system. The vulnerability is present in versions 9.0.2.0 and earlier. Oracle has released a patch for this vulnerability. Users are advised to upgrade to the latest version of the software.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Hospitality Cruise Fleet Management	9.0.2.0	All	All	All
Application	Oracle	Hospitality Cruise Fleet Management	9.0.2.0	All	All	All

References

Reference	Source	Link	Tags
Oracle Hospitality Cruise Fleet Management CVE-2017-10397 Remote Security Vulnerability	BID	www.securityfocus.com	
Oracle Critical Patch Update - October 2017	CONFIRM	www.oracle.com	Patch, CVE-2017-10397
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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