CVE-2014-6476

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-6476
State	PUBLIC
Assigner	secalert_us@oracle.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-15 15:55:00 UTC
Updated	2020-09-08 13:00:00 UTC
Description	Unspecified vulnerability in Oracle Java SE 7u67 and 8u20 allows remote attackers to affect integrity via unknown vectors r

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Oracle	Jdk	1.7.0	update67	All	All
Application	Oracle	Jdk	1.8.0	update20	All	All
Application	Oracle	Jdk	1.7.0	update67	All	All
Application	Oracle	Jdk	1.8.0	update20	All	All
Application	Oracle	Jre	1.7.0	update_67	All	All
Application	Oracle	Jre	1.8.0	update_20	All	All
Application	Oracle	Jre	1.7.0	update_67	All	All
Application	Oracle	Jre	1.8.0	update_20	All	All

References

Reference	Source
[security-announce] SUSE-SU-2014:1526-1: important: Security update for	SUSE
Red Hat Customer Portal	REDHAT
Oracle Java SE CVE-2014-6476 Remote Security Vulnerability	BID
Red Hat Customer Portal	REDHAT
[security-announce] SUSE-SU-2015:0344-1: important: Security update for	SUSE
'[security bulletin] HPSBUX03218 SSRT101770 rev.1 - HP-UX running Java7, Remote Unauthorized Access, ' - MARC	HP

Red Hat Customer Portal	REDHAT
Oracle JRE/JDK: Multiple vulnerabilities (GLSA 201502-12) — Gentoo security	GENTOO
Red Hat Customer Portal	REDHAT
IBM Security Bulletin: Multiple vulnerabilities in current releases of the IBM® SDK, Java™ Technology Edition - United States	CONFIRM
[security-announce] SUSE-SU-2014:1549-1: important: Security update for	SUSE
About Secunia Research | Flexera	SECUNIA
Oracle Critical Patch Update - October 2014	CONFIRM
About Secunia Research | Flexera	SECUNIA
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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