CVE-2014-7968

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

Summary

CVE	CVE-2014-7968
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-10-22 14:55:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	VDSM allows remote attackers to cause a denial of service (connection blocking) by keeping an SSL connection open.

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:P

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Virtual Desktop Service Manager	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
oss-security - CVE request for VDSM denial of service	af854a3a-2127-422b-91ae-364da266
Bug 1150812 – CVE-2014-7968 vdsm: ssl_accept may block connections on uncompleted handshake	af854a3a-2127-422b-91ae-364da266
oss-security - Re: CVE request for VDSM denial of service / oVirt	af854a3a-2127-422b-91ae-364da266
oss-security - Re: CVE request for VDSM denial of service	af854a3a-2127-422b-91ae-364da266
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.