CVE-2015-3247

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-3247
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-09-08 15:59:00 UTC
Updated	2023-02-12 23:15:00 UTC
Description	Race condition in the worker_update_monitors_config function in SPICE 0.12.4 allows a remote authenticated guest user to

Risk And Classification

Problem Types: CWE-119 | CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Application	Spice Project	Spice	0.12.4	All	All	All
Application	Spice Project	Spice	0.12.4	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Customer Portal
Bug 1233238 – CVE-2015-3247 spice: memory corruption in worker_update_monitors_config()
Spice Memory Corruption Error in worker_update_monitors_config() Lets Local Users on a Guest System Gain Elevated Privileges on the Hos
Debian -- Security Information -- DSA-3354-1 spice
Red Hat Enterprise Virtualization Hypervisor Bugs Let Remote Users Execute Arbitrary Code, Gain Elevated Privileges, and Deny Service - S
Red Hat Customer Portal
Spice Race Condition and Buffer Overflows Let Local Guest System Users Crash the Host or Execute Arbitrary Code on the Host System - Se
[Spice-devel] Announcing spice 0.12.6
Red Hat Customer Portal
access.redhat.com | CVE-2015-3247
openSUSE-SU-2015:1566-1: moderate: Security update for spice
Red Hat Customer Portal
USN-2736-1: Spice vulnerability | Ubuntu
Red Hat Customer Portal
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

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