CVE-2011-1179

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

Summary

CVE	CVE-2011-1179
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-04-18 17:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SPICE Firefox plug-in (spice-xpi) 2.4, 2.3, 2.2, and possibly other versions allows remote attackers to cause a denial of

Risk And Classification

Primary CVSS: v2.0 5.1 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mozilla	Firefox	All	All	All	All

Application	Redhat	Spice-xpi	2.2	All	All	All
Application	Redhat	Spice-xpi	2.3	All	All	All
Application	Redhat	Spice-xpi	2.4	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Support	af854a3a-2
Attachment 487006 Details for Bug 689931 – Resolution of the security issue (nsPluginInstance, getters and setters)	af854a3a-2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2
Red Hat Spice-xpi Bugs Let Local Users Gain Elevated Privileges and Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2
689931 – (CVE-2011-1179) CVE-2011-1179 spice-xpi: unitialized pointer writes possible when getting plugin properties	af854a3a-2
Support	af854a3a-2
IBM X-Force Exchange	af854a3a-2
Malformed Request	af854a3a-2
Red Hat update for spice-xpi - Secunia.com	af854a3a-2
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.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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 registred 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**