



CVE-2011-0904

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

Summary

CVE	CVE-2011-0904
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-10 18:55:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The rfbSendFramebufferUpdate function in server/libvncserver/rfbserver.c in vino-server in Vino 2.x before 2.28.3, 2.32.x before 2.32.1, and 2.32.2 before 2.32.2.1 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a crafted RFB packet.

Risk And Classification

Primary CVSS: v2.0 3.5 from nvd@nist.gov

AV:N/AC:M/Au:S/C:N/I:N/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:M/Au:S/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	David King	Vino	2.10	All	All	All

Application	David King	Vino	2.11	All	All	All
Application	David King	Vino	2.12	All	All	All
Application	David King	Vino	2.13	All	All	All
Application	David King	Vino	2.13.5	All	All	All
Application	David King	Vino	2.14	All	All	All
Application	David King	Vino	2.15	All	All	All
Application	David King	Vino	2.16	All	All	All
Application	David King	Vino	2.17	All	All	All
Application	David King	Vino	2.17.2	All	All	All
Application	David King	Vino	2.17.4	All	All	All
Application	David King	Vino	2.17.5	All	All	All
Application	David King	Vino	2.17.92	All	All	All
Application	David King	Vino	2.18	All	All	All
Application	David King	Vino	2.18.1	All	All	All
Application	David King	Vino	2.19	All	All	All
Application	David King	Vino	2.19.5	All	All	All
Application	David King	Vino	2.19.90	All	All	All
Application	David King	Vino	2.19.92	All	All	All
Application	David King	Vino	2.20	All	All	All
Application	David King	Vino	2.20.1	All	All	All
Application	David King	Vino	2.21	All	All	All
Application	David King	Vino	2.21.1	All	All	All
Application	David King	Vino	2.21.2	All	All	All
Application	David King	Vino	2.21.3	All	All	All
Application	David King	Vino	2.21.90	All	All	All
Application	David King	Vino	2.21.91	All	All	All
Application	David King	Vino	2.21.92	All	All	All
Application	David King	Vino	2.22	All	All	All
Application	David King	Vino	2.22.1	All	All	All
Application	David King	Vino	2.22.2	All	All	All
Application	David King	Vino	2.23	All	All	All
Application	David King	Vino	2.23.5	All	All	All
Application	David King	Vino	2.23.90	All	All	All
Application	David King	Vino	2.23.91	All	All	All
Application	David King	Vino	2.23.92	All	All	All
Application	David King	Vino	2.24	All	All	All

Application	David King	Vino	2.24.1	All	All	All
Application	David King	Vino	2.25	All	All	All
Application	David King	Vino	2.25.3	All	All	All
Application	David King	Vino	2.25.4	All	All	All
Application	David King	Vino	2.25.5	All	All	All
Application	David King	Vino	2.25.90	All	All	All
Application	David King	Vino	2.25.91	All	All	All
Application	David King	Vino	2.25.92	All	All	All
Application	David King	Vino	2.26	All	All	All
Application	David King	Vino	2.26.1	All	All	All
Application	David King	Vino	2.26.2	All	All	All
Application	David King	Vino	2.27	All	All	All
Application	David King	Vino	2.27.5	All	All	All
Application	David King	Vino	2.27.90	All	All	All
Application	David King	Vino	2.27.91	All	All	All
Application	David King	Vino	2.27.92	All	All	All
Application	David King	Vino	2.28	All	All	All
Application	David King	Vino	2.28.1	All	All	All
Application	David King	Vino	2.28.2	All	All	All
Application	David King	Vino	2.32.0	All	All	All
Application	David King	Vino	2.32.1	All	All	All
Application	David King	Vino	2.7	All	All	All
Application	David King	Vino	2.7.3	All	All	All
Application	David King	Vino	2.7.3.1	All	All	All
Application	David King	Vino	2.7.4	All	All	All
Application	David King	Vino	2.7.4.90	All	All	All
Application	David King	Vino	2.7.4.91	All	All	All
Application	David King	Vino	2.7.92	All	All	All
Application	David King	Vino	2.8	All	All	All
Application	David King	Vino	2.9	All	All	All
Application	David King	Vino	2.9.2	All	All	All
Application	David King	Vino	3.0.0	All	All	All
Application	David King	Vino	3.0.1	All	All	All
Application	David King	Vino	3.1	All	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference				
IBM X-Force Exchange				
694455 – (CVE-2011-0904) CVE-2011-0904 vino: Out of bounds read flaw by processing certain client raw encoding framebuffer update requ				
NEWS · master · Archive / vino · GitLab				
Commits · gnome-2-30 · Archive / vino · GitLab				
Update NEWS for 3.1.1 release (d050a22b) · Commits · Archive / vino · GitLab				
ftp.gnome.org/pub/GNOME/sources/vino/2.32/vino-2.32.2.news				
Red Hat Customer Portal				
Avoid out-of-bounds memory accesses (dff52694) · Commits · Archive / vino · GitLab				
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:009				
ftp.gnome.org/pub/GNOME/sources/vino/2.28/vino-2.28.3.news				
Ubuntu update for vino - Advisories - Community				
Debian -- Security Information -- DSA-2238-1 vino				
Avoid out-of-bounds memory accesses (e17bd4e3) · Commits · Archive / vino · GitLab				
Avoid out-of-bounds memory accesses (456dadbb) · Commits · Archive / vino · GitLab				
Bug 641802 – Vino 2.26.1 and 2.32.1 allows remote attackers to trigger an out-of-bounds write				
USN-1128-1: Vino vulnerabilities Ubuntu				
mandriva.com				
Avoid out-of-bounds memory accesses (8beefcf7) · Commits · Archive / vino · GitLab				
Security Advisory SA44463 - Vino Framebuffer Update Handling Denial of Service Vulnerability - Secunia				
Vino Framebuffer Request Processing Multiple Remote Denial of Service Vulnerabilities				
ftp.gnome.org/pub/GNOME/sources/vino/3.0/vino-3.0.2.news				
Avoid out-of-bounds memory accesses (0c2c9175) · Commits · Archive / vino · GitLab				
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](#) 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 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](#)