



# CVE-2010-2643

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2010-2643
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2011-01-07 19:00:00 UTC
<b>Updated</b>	2012-01-19 03:49:00 UTC
<b>Description</b>	Integer overflow in the TFM font parser in the dvi-backend component in Evince 2.32 and earlier allows remote attackers to

## Risk And Classification

### Problem Types: CWE-189

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Evince	0.1	All	All	All
Application	Redhat	Evince	0.2	All	All	All
Application	Redhat	Evince	0.3	All	All	All
Application	Redhat	Evince	0.4	All	All	All
Application	Redhat	Evince	0.5	All	All	All
Application	Redhat	Evince	0.6	All	All	All
Application	Redhat	Evince	0.7	All	All	All
Application	Redhat	Evince	0.8	All	All	All
Application	Redhat	Evince	0.9	All	All	All
Application	Redhat	Evince	2.19	All	All	All
Application	Redhat	Evince	2.20	All	All	All
Application	Redhat	Evince	2.21	All	All	All
Application	Redhat	Evince	2.22	All	All	All
Application	Redhat	Evince	2.23	All	All	All
Application	Redhat	Evince	2.24	All	All	All
Application	Redhat	Evince	2.25	All	All	All
Application	Redhat	Evince	2.26	All	All	All

Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.27	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.28	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.29	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.29.92	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.4.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.6	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.6.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.90	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.92	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.32	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.5	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.6	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.7	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.8	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	0.9	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.19	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.20	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.21	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.22	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.23	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.24	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.25	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.26	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.27	All	All	All

Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.28	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.29	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.29.92	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.30.3	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.2	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.4	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.4.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.6	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.6.1	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.90	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.31.92	All	All	All
Application	<a href="#">Redhat</a>	<a href="#">Evince</a>	2.32	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 13 Update: evince-2.30.3-2.fc13	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Red Hat update for evince - Advisories - Community	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Debian -- Security Information -- DSA-2357-1 evince	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Evince dvi-backend Multiple Vulnerabilities - Advisories - Community	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Ubuntu update for evince - Advisories - Community	SECUNIA	<a href="https://secunia.com">secunia.com</a>
Evince Multiple Remote Code Execution Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
USN-1035-1: Evince vulnerabilities   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
Bug 666321 – CVE-2010-2643 evince: Integer overflow in DVI file TFM font parser	CONFIRM	<a href="https://bugzilla.redhat.com">bugzilla.redhat.com</a>
Evince Font Parsing Buffer Overflows Let Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
evince - View multipage documents	CONFIRM	<a href="https://git.gnome.org">git.gnome.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
[SECURITY] Fedora 14 Update: evince-2.32.0-3.fc14	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
rhn.redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Fedora update for evince - Advisories - Community	SECUNIA	<a href="https://secunia.com">secunia.com</a>

mandriva.com	MANDRIVA	<a href="https://lists.mandriva.com">lists.mandriva.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="https://www.vupen.com">www.vupen.com</a>
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:002	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="https://www.vupen.com">www.vupen.com</a>
SUSE update for Multiple Packages - Secunia.com	SECUNIA	<a href="https://secunia.com">secunia.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses).

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)