



# CVE-2017-6312

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-6312
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-10 02:59:00 UTC
<b>Updated</b>	2023-11-07 02:49:00 UTC
<b>Description</b>	Integer overflow in io-ico.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (segmentation fault)

## Risk And Classification

**Problem Types:** CWE-190

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	30	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	31	All	All	All
Application	<a href="#">Gnome</a>	<a href="#">Gdk-pixbuf</a>	All	All	All	All
Application	<a href="#">Gnome</a>	<a href="#">Gdk-pixbuf</a>	All	All	All	All

## References

Reference	Source	Link
Bug hunting GDK-PixBuf   mov.sx	MISC	<a href="#">mov.sx</a>
oss-security - Re: CVE Request - Multiple vulnerabilities in gdk-pixbuf	MLIST	<a href="#">www.openwall.com</a>
[SECURITY] Fedora 30 Update: mingw-gdk-pixbuf-2.36.12-1.fc30 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] Fedora 31 Update: mingw-gdk-pixbuf-2.40.0-1.fc31 - package-announce - Fedora Mailing-Lists		<a href="#">lists.fedoraproject.org</a>
[SECURITY] [DLA 2043-1] gdk-pixbuf security update	MLIST	<a href="#">lists.debian.org</a>
GDK-PixBuf: Multiple vulnerabilities (GLSA 201709-08) — Gentoo security	GENTOO	<a href="#">security.gentoo.org</a>

[SECURITY] Fedora 30 Update: mingw-gdk-pixbuf-2.36.12-1.fc30 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
oss-security - CVE Request - Multiple vulnerabilities in gdk-pixbuf	MLIST	<a href="https://www.openwall.com">www.openwall.com</a>
[SECURITY] Fedora 31 Update: mingw-gdk-pixbuf-2.40.0-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	<a href="https://lists.fedoraproject.org">lists.fedoraproject.org</a>
Bug 779012 – Possible out-of-bounds read or undefined behavior in io-ico.c	MISC	<a href="https://bugzilla.gnome.org">bugzilla.gnome.org</a>
gdk-pixbuf Integer Overflow and Denial of Service Vulnerabilities	BID	<a href="https://www.securityfocus.com">www.securityfocus.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.

### Legacy QID Mappings

- [500199](#) Alpine Linux Security Update for gdk-pixbuf
- [503941](#) Alpine Linux Security Update for gdk-pixbuf
- [710335](#) Gentoo Linux GDK-PixBuf Multiple Vulnerabilities (GLSA 201709-08)

© [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](#).

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