



CVE-2018-7436

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

Summary

CVE	CVE-2018-7436
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-23 21:29:00 UTC
Updated	2023-11-07 03:01:00 UTC
Description	An issue was discovered in FreeXL before 1.0.5. There is a heap-based buffer over-read in a pointer dereference of the pa

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Freexl Project	Freexl	All	All	All	All
Application	Freexl Project	Freexl	All	All	All	All

References

Reference	Source	Link	Tags
FreeXL: Multiple vulnerabilities (GLSA 202007-44) — Gentoo security	GENTOO	security.gentoo.org	
Google Groups		groups.google.com	
[SECURITY] [DLA 1297-1] freexl security update	MLIST	lists.debian.org	Mailing List, Third Party Advisor
Debian -- Security Information -- DSA-4129-1 freexl	DEBIAN	www.debian.org	Third Party Advisory
Google Groups	MISC	groups.google.com	Exploit, Third Party Advisory
1547883 – heap-buffer-overflow in freexl.c:1805 parse_SST parse_SST	MISC	bugzilla.redhat.com	Exploit, Issue Tracking, Third Party

CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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