



CVE-2012-1051

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

Summary

CVE	CVE-2012-1051
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-02-13 19:55:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	Heap-based buffer overflow in Xjp2.dll in the JPEG2000 plug-in in XnView 1.98.5 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via crafted JPEG2000 image, as demonstrated by a proof of concept exploit.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Xnview	Xnview	1.98.5	All	All	All
Application	Xnview	Xnview	1.98.5	All	All	All

References

Reference	Source	Link
XnView JPEG2000 Buffer Overflow Vulnerability	BID	www.securityfocus.com
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com
Security Advisory SA47352 - XnView Image Processing Buffer Overflow Vulnerabilities - Secunia	SECUNIA	secunia.com
78904	OSVDB	osvdb.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)