



# CVE-2006-2909

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

## Summary

<b>CVE</b>	CVE-2006-2909
<b>State</b>	PUBLIC
<b>Assigner</b>	PSIRT-CNA@flexerasoftware.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-06-16 10:02:00 UTC
<b>Updated</b>	2018-10-18 16:43:00 UTC
<b>Description</b>	Stack-based buffer overflow in the info tip shell extension (zipinfo.dll) in PicoZip 4.01 allows remote attackers to execute arbitrary code.

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Picozip</a>	<a href="#">Picozip</a>	4.01	All	All	All
Application	<a href="#">Picozip</a>	<a href="#">Picozip</a>	4.01	All	All	All

## References

Reference	Source	Link
PicoZip Zipinfo.DLL Buffer Overflow Vulnerability	BID	<a href="#">www.se</a>
SecurityTracker.com Archives - PicoZip 'zipinfo.dll' Buffer Overflow Lets Remote Users Execute Arbitrary Code	SECTRACK	<a href="#">security</a>
26447	OSVDB	<a href="#">www.os</a>
IBM X-Force Exchange	XF	<a href="#">exchang</a>
PicoZip "zipinfo.dll" Multiple Archives Buffer Overflow - Secunia Research - Secunia	MISC	<a href="#">secunia</a>
SecurityFocus	BUGTRAQ	<a href="#">www.se</a>
SecurityFocus	BUGTRAQ	<a href="#">www.se</a>
SecurityReason - Secunia Research: PicoZip "zipinfo.dll" Multiple Archives BufferOverflow	SREASON	<a href="#">security</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.vu</a>
PicoZip "zipinfo.dll" Multiple Archives Buffer Overflow - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="#">secunia</a>
Zip and Unzip Compressed Files Easily - PicoZip	CONFIRM	<a href="#">www.pic</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</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](#).

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