



CVE-2006-0855

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2006-0855
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-23 21:02:00 UTC
Updated	2018-10-18 16:29:00 UTC
Description	Stack-based buffer overflow in the fullpath function in misc.c for zoo 2.10 and earlier, as used in products such as Barracud

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Rahul Dhesi	Zoo	All	All	All	All

References

Reference

Barracuda Spam Firewall Archives Buffer Overflow Vulnerabilities - Advisories - Secunia

SecurityReason

Debian -- Security Information -- DSA-991-1 zoo

Webmail - OVH

Debian update for zoo - Advisories - Secunia

Gentoo update for zoo - Advisories - Secunia

Gentoo Linux Documentation -- zoo: Stack-based buffer overflow

Zoo "fullpath()" File Name Handling Buffer Overflow - Advisories - Secunia

20060403 Barracuda ZOO archiver security bug leads to remote compromise

Zoo Misc.c Buffer Overflow Vulnerability

Webmail - OVH

Security Announcement

SecurityFocus

SUSE Updates for Multiple Packages - Advisories - Secunia

IBM X-Force Exchange

www.guay-leroux.com/projects/zoo-advisory.txt

SUSE Updates for Multiple Packages - Advisories - Secunia

www.guay-leroux.com/projects/barracuda-advisory-ZOO.txt

Security Announcement

zoo Buffer Overflow in fullpath() Lets Remote Users Cause Arbitrary Code to Be Executed - SecurityTracker

Barracuda Spam Firewall Buffer Overflows in Processing LHA and ZOO Archives Let Remote Users Execute Arbitrary Code - SecurityTracker

CVE Program record

NVD vulnerability detail



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