



CVE-2006-1953

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2006-1953
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-05-17 10:06:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Directory traversal vulnerability in Caucho Resin 3.0.17 and 3.0.18 for Windows allows remote attackers to read arbitrary files

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:N/A:N

EPSS: 0.009100000 probability, percentile 0.758360000 (date 2026-04-20)

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:C/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Caucho Technology	Resin	3.0.17	All	windows	All
Application	Caucho Technology	Resin	3.0.18	All	windows	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

About Secunia Research | Flexera

archives.neohapsis.com/archives/vulnwatch/2006-q2/0026.html

www.osvdb.org/25570

Caucho Resin Remote Directory Traversal Vulnerability

IBM X-Force Exchange

Resin Input Validation Flaw in the Built-in Web Server Lets Remote Users Traverse the Directory By Specifying an Absolute Path - SecurityTrails

SecurityFocus

Rapid7 Security Advisory R7-0024: Caucho Resin Windows Directory Traversal Vulnerability

Caucho Resin Windows Directory Traversal Vulnerability - SecurityReason.com

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](#) 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