CVE-2008-4695

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-4695
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-10-23 22:00:01 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Opera before 9.60 allows remote attackers to obtain sensitive information and have unspecified other impact by predicting t

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-200 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opera	Opera	5.0	All	All	All

Application	Opera	Opera	5.0	beta_2	All	All
Application	Opera	Opera	5.0	beta_3	All	All
Application	Opera	Opera	5.0	beta_4	All	All
Application	Opera	Opera	5.0	beta_5	All	All
Application	Opera	Opera	5.0	beta_6	All	All
Application	Opera	Opera	5.0	beta_7	All	All
Application	Opera	Opera	5.0	beta_8	All	All
Application	Opera	Opera	5.02	All	All	All
Application	Opera	Opera	5.10	All	All	All
Application	Opera	Opera	5.11	All	All	All
Application	Opera	Opera	5.12	All	All	All
Application	Opera	Opera	6.0	All	All	All
Application	Opera	Opera	6.0	beta_1	All	All
Application	Opera	Opera	6.0	beta_2	All	All
Application	Opera	Opera	6.0	beta_3	All	All
Application	Opera	Opera	6.01	All	All	All
Application	Opera	Opera	6.02	All	All	All
Application	Opera	Opera	6.03	All	All	All
Application	Opera	Opera	6.04	All	All	All
Application	Opera	Opera	6.05	All	All	All
Application	Opera	Opera	6.06	All	All	All
Application	Opera	Opera	6.1	All	All	All
Application	Opera	Opera	6.11	All	All	All
Application	Opera	Opera	6.12	All	All	All
Application	Opera	Opera	7.0	All	All	All
Application	Opera	Opera	7.0	beta_1	All	All
Application	Opera	Opera	7.0	beta_1v2	All	All
Application	Opera	Opera	7.0	beta_2	All	All
Application	Opera	Opera	7.01	All	All	All
Application	Opera	Opera	7.02	All	All	All
Application	Opera	Opera	7.03	All	All	All
Application	Opera	Opera	7.10	All	All	All
Application	Opera	Opera	7.11	All	All	All
Application	Opera	Opera	7.20	All	All	All
Application	Opera	Opera	7.20	beta7	All	All
Application	Opera	Opera	7.21	All	All	All

Application	Opera	Opera	7.22	All	All	All
Application	Opera	Opera	7.23	All	All	All
Application	Opera	Opera	7.50	All	All	All
Application	Opera	Opera	7.50	beta_1	All	All
Application	Opera	Opera	7.51	All	All	All
Application	Opera	Opera	7.52	All	All	All
Application	Opera	Opera	7.53	All	All	All
Application	Opera	Opera	7.54	All	All	All
Application	Opera	Opera	7.54	update_1	All	All
Application	Opera	Opera	7.54	update_2	All	All
Application	Opera	Opera	8.0	All	All	All
Application	Opera	Opera	8.0	beta_1	All	All
Application	Opera	Opera	8.0	beta_2	All	All
Application	Opera	Opera	8.0	beta_3	All	All
Application	Opera	Opera	8.01	All	All	All
Application	Opera	Opera	8.02	All	All	All
Application	Opera	Opera	8.50	All	All	All
Application	Opera	Opera	8.51	All	All	All
Application	Opera	Opera	8.52	All	All	All
Application	Opera	Opera	8.53	All	All	All
Application	Opera	Opera	8.54	All	All	All
Application	Opera	Opera	9.0	All	All	All
Application	Opera	Opera	9.0	beta_1	All	All
Application	Opera	Opera	9.0	beta_2	All	All
Application	Opera	Opera	9.01	All	All	All
Application	Opera	Opera	9.02	All	All	All
Application	Opera	Opera	9.10	All	All	All
Application	Opera	Opera	9.20	All	All	All
Application	Opera	Opera	9.20	beta_1	All	All
Application	Opera	Opera	9.21	All	All	All
Application	Opera	Opera	9.22	All	All	All
Application	Opera	Opera	9.23	All	All	All
Application	Opera	Opera	9.24	All	All	All
Application	Opera	Opera	9.25	All	All	All
Application	Opera	Opera	9.26	All	All	All

Application	Opera	Opera	9.27	All	All	All
Application	Opera	Opera	9.50	All	All	All
Application	Opera	Opera	9.50	beta_1	All	All
Application	Opera	Opera	9.50	beta_2	All	All
Application	Opera	Opera	9.51	All	All	All
Application	Opera	Opera	9.52	All	All	All
Application	Opera	Opera	All	beta_1	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Opera 9.6 for Linux Changelog	af854a3a-2127-422b-91ae-364da26611
Advisory: Java applets can be used to read sensitive information - Opera Knowledge Base	af854a3a-2127-422b-91ae-364da26611
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da26611
Opera Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da26611
Opera Cached Java Applet Security Bypass Vulnerability	af854a3a-2127-422b-91ae-364da26611
Gentoo update for opera - Secunia.com	af854a3a-2127-422b-91ae-364da26611
oss-security - Re: CVE Request: Opera 9.60 with security fixes	af854a3a-2127-422b-91ae-364da26611
Opera 9.6 for Windows Changelog	af854a3a-2127-422b-91ae-364da26611
Opera Java Applet Processing Bug Lets Remote Users Access Cached Files - SecurityTracker	af854a3a-2127-422b-91ae-364da26611
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da26611
Gentoo Linux Documentation -- Opera: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da26611
Opera 9.6 for Solaris Changelog	af854a3a-2127-422b-91ae-364da26611
Opera 9.6 for FreeBSD Changelog	af854a3a-2127-422b-91ae-364da26611
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:022	af854a3a-2127-422b-91ae-364da26611
Opera 9.6 for Mac Changelog	af854a3a-2127-422b-91ae-364da26611
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da26611
oss-security - CVE Request: Opera 9.60 with security fixes	af854a3a-2127-422b-91ae-364da26611
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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 registred 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**