



CVE-2008-5679

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

Summary

CVE	CVE-2008-5679
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-19 16:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The HTML parsing engine in Opera before 9.63 allows remote attackers to execute arbitrary code via crafted web pages that

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-399 | 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	All	All	All	All

Application	Opera	Opera	5..10	All	All	All
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	5.1	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	5.2	All	All	All
Application	Opera	Opera	5.3	All	All	All
Application	Opera	Opera	5.4	All	All	All
Application	Opera	Opera	5.5	All	All	All
Application	Opera	Opera	5.6	All	All	All
Application	Opera	Opera	5.7	All	All	All
Application	Opera	Opera	5.8	All	All	All
Application	Opera	Opera	5.9	All	All	All
Application	Opera	Opera	6	beta_1	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	beta_1	All	All
Application	Opera	Opera	7	beta_1.2	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	9.6	All	All	All
Application	Opera	Opera	9.60	All	All	All
Application	Opera	Opera	9.60	beta_1	All	All
Application	Opera	Opera	9.61	All	All	All
Application	Opera	Opera	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
SecurityFocus	af854a3a-2127-422b-91ae-364da266110
Opera 9.63 for Linux Changelog	af854a3a-2127-422b-91ae-364da266110
Gentoo Linux Documentation -- Opera: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da266110
Advisory: HTML parsing flaw can cause Opera to execute arbitrary code - Opera Knowledge Base	af854a3a-2127-422b-91ae-364da266110

Best 7 Best Internet Security Software in 2019	af854a3a-2127-422b-91ae-364da266110
Gentoo update for opera - Advisories - Community	af854a3a-2127-422b-91ae-364da266110
Opera HTML Parsing Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da266110
n.runs-SA-2008.010 - Opera HTML parsing Code Execution - CXSecurity.com	af854a3a-2127-422b-91ae-364da266110
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 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](#)