CVE-2008-5178

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

Summary

CVE	CVE-2008-5178
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-11-20 15:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Heap-based buffer overflow in Opera 9.62 on Windows allows remote attackers to execute arbitrary code via a long file:// U

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-119 | 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
Operating System	Microsoft	Windows	All	All	All	All

Application	Opera	Opera	9.62	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
Opera Multiple Vulnerabilities - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-91ae-364da2
Gentoo Linux Documentation -- Opera: Multiple vulnerabilities	af854a3a-2127-422b-91ae-364da2
Opera 9.62 file:// Local Heap Overflow Exploit	af854a3a-2127-422b-91ae-364da2
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2
osvdb.org/49882	af854a3a-2127-422b-91ae-364da2
Opera Web Browser 'file://' Heap Based Buffer Overflow Vulnerability	af854a3a-2127-422b-91ae-364da2
archives.neohapsis.com/archives/bugtraq/2008-11/0110.html	af854a3a-2127-422b-91ae-364da2
Advisory: Long hostnames in file: URLs can cause execution of arbitrary code - Opera Knowledge Base	af854a3a-2127-422b-91ae-364da2
Gentoo update for opera - Advisories - Community	af854a3a-2127-422b-91ae-364da2
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.