



CVE-2008-5905

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

Summary

CVE	CVE-2008-5905
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-15 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The web interface plugin in KTorrent before 3.1.4 allows remote attackers to bypass intended access restrictions and upload files to the local system.

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-264 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ktorrent	Ktorrent	0.9	All	All	All

Application	Ktorrent	Ktorrent	1.0	All	All	All
Application	Ktorrent	Ktorrent	1.1	All	All	All
Application	Ktorrent	Ktorrent	1.2	All	All	All
Application	Ktorrent	Ktorrent	1.2	rc1	All	All
Application	Ktorrent	Ktorrent	1.2	rc2	All	All
Application	Ktorrent	Ktorrent	2.0	All	All	All
Application	Ktorrent	Ktorrent	2.0	beta1	All	All
Application	Ktorrent	Ktorrent	2.0	rc1	All	All
Application	Ktorrent	Ktorrent	2.0.1	All	All	All
Application	Ktorrent	Ktorrent	2.0.2	All	All	All
Application	Ktorrent	Ktorrent	2.0.3	All	All	All
Application	Ktorrent	Ktorrent	2.1	All	All	All
Application	Ktorrent	Ktorrent	2.1	beta1	All	All
Application	Ktorrent	Ktorrent	2.1	rc1	All	All
Application	Ktorrent	Ktorrent	2.1.1	All	All	All
Application	Ktorrent	Ktorrent	2.1.2	All	All	All
Application	Ktorrent	Ktorrent	2.1.3	All	All	All
Application	Ktorrent	Ktorrent	2.1.4	All	All	All
Application	Ktorrent	Ktorrent	2.2	All	All	All
Application	Ktorrent	Ktorrent	2.2	beta1	All	All
Application	Ktorrent	Ktorrent	2.2	rc1	All	All
Application	Ktorrent	Ktorrent	2.2.1	All	All	All
Application	Ktorrent	Ktorrent	2.2.2	All	All	All
Application	Ktorrent	Ktorrent	2.2.3	All	All	All
Application	Ktorrent	Ktorrent	2.2.4	All	All	All
Application	Ktorrent	Ktorrent	2.2.5	All	All	All
Application	Ktorrent	Ktorrent	2.2.6	All	All	All
Application	Ktorrent	Ktorrent	2.2.7	All	All	All
Application	Ktorrent	Ktorrent	2.2.8	All	All	All
Application	Ktorrent	Ktorrent	3.0	beta1	All	All
Application	Ktorrent	Ktorrent	3.0	rc1	All	All
Application	Ktorrent	Ktorrent	3.0.0	All	All	All
Application	Ktorrent	Ktorrent	3.0.1	All	All	All
Application	Ktorrent	Ktorrent	3.0.2	All	All	All
Application	Ktorrent	Ktorrent	3.1.1	All	All	All
Application	Ktorrent	Ktorrent	3.1.2	All	All	All

Application	Ktorrent	Ktorrent	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		
KTorrent 2 Web Interface Torrent Upload and PHP Code Injection - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-		
Gentoo Linux Documentation -- KTorrent: Multiple vulnerabilitites				af854a3a-		
Gentoo Bug 244741 - net-p2p/ktorrent <2.2.8 web interface plugin vulnerable to PHP injection (CVE-2008-{5905,5906})				af854a3a-		
#504178 - KTorrent Web Interface Torrent Upload and PHP Code Injection - Debian Bug report logs				af854a3a-		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-		
USN-711-1: KTorrent vulnerabilities Ubuntu				af854a3a-		
Gentoo update for ktorrent - Secunia Advisories - Vulnerability Information - Secunia.com				af854a3a-		
KTorrent PHP Code Injection And Security Bypass Vulnerabilities				af854a3a-		
Ubuntu update for ktorrent - Secunia.com				af854a3a-		
KTorrent Web Interface Torrent Upload and PHP Code Injection - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-		
IBM X-Force Exchange				af854a3a-		
oss-security - CVE request: ktorrent				af854a3a-		
3.1.4 released KTorrent				af854a3a-		
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.						