



CVE-2009-2534

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

Summary

CVE	CVE-2009-2534
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-20 17:30:00 UTC
Updated	2018-10-10 19:40:00 UTC
Description	RealNetworks Helix Server and Helix Mobile Server before 13.0.0 allow remote attackers to cause a denial of service (daemon crash) by sending a crafted RTSP SETUP request.

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Server	11.0	All	All	All
Application	Realnetworks	Helix Server	12.0.0	All	All	All
Application	Realnetworks	Helix Server	11.0	All	All	All
Application	Realnetworks	Helix Server	12.0.0	All	All	All
Application	Realnetworks	Helix Server	All	All	All	All
Application	Realnetworks	Helix Server Mobile	11.0	All	All	All
Application	Realnetworks	Helix Server Mobile	11.0	All	All	All
Application	Realnetworks	Helix Server Mobile	All	All	All	All

References

Reference	Source	Link	Tags
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com	
Real Helix DNA RTSP and SETUP Request Handler Vulnerabilities	EXPLOIT-DB	www.exploit-db.com	
55982	OSVDB	osvdb.org	
RealNetworks Helix Server 'SETUP' Remote Denial of Service Vulnerability	BID	www.securityfocus.com	
SecurityFocus	BUGTRAQ	www.securityfocus.com	
Core Security Technologies	MISC	www.coresecurity.com	Exploit

docs.real.com/docs/security/SecurityUpdate071409HS.pdf	CONFIRM	docs.real.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](https://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