



CVE-2010-1318

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

Summary

CVE	CVE-2010-1318
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-04-20 15:30:00 UTC
Updated	2010-11-24 05:00:00 UTC
Description	Stack-based buffer overflow in the AgentX::receive_agentx function in AgentX++ 1.4.16, as used in RealNetworks Helix Ser

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Mobile Server	All	All	All	All
Application	Realnetworks	Helix Server	11.0	All	All	All
Application	Realnetworks	Helix Server	11.1	All	All	All
Application	Realnetworks	Helix Server	12.0.0	All	All	All
Application	Realnetworks	Helix Server	12.0.1	All	All	All
Application	Realnetworks	Helix Server	11.0	All	All	All
Application	Realnetworks	Helix Server	11.1	All	All	All
Application	Realnetworks	Helix Server	12.0.0	All	All	All
Application	Realnetworks	Helix Server	12.0.1	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	12.0.0	All	All	All
Application	Realnetworks	Helix Server Mobile	13.0.0	All	All	All
Application	Realnetworks	Helix Server Mobile	11.0	All	All	All
Application	Realnetworks	Helix Server Mobile	12.0.0	All	All	All
Application	Realnetworks	Helix Server Mobile	13.0.0	All	All	All

References		
Reference	Source	Link
404 Realnetworks	CONFIRM	www.realnetworks.com
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
Helix Server and Helix Mobile Server Multiple Vulnerabilities - Advisories - Community	SECUNIA	secunia.com
RealNetworks Helix and Helix Mobile Server NTLM Authentication Heap Buffer Overflow Vulnerability	BID	www.securityfocus.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
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](#)