CVE-2007-4561

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

Summary

CVE	CVE-2007-4561
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-28 01:17:00 UTC
Updated	2011-03-08 02:58:00 UTC
Description	Heap-based buffer overflow in the RTSP service in Helix DNA Server before 11.1.4 allows remote attackers to execute arbi

Risk And Classification

Problem Types: CWE-119 | CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Realnetworks	Helix Dna Server	10.0	All	All	All
Application	Realnetworks	Helix Dna Server	11.0	All	All	All
Application	Realnetworks	Helix Dna Server	11.1	All	All	All
Application	Realnetworks	Helix Dna Server	11.1.2	All	All	All
Application	Realnetworks	Helix Dna Server	11.1.3	All	All	All
Application	Realnetworks	Helix Dna Server	10.0	All	All	All
Application	Realnetworks	Helix Dna Server	11.0	All	All	All
Application	Realnetworks	Helix Dna Server	11.1	All	All	All
Application	Realnetworks	Helix Dna Server	11.1.2	All	All	All
Application	Realnetworks	Helix Dna Server	11.1.3	All	All	All

References

Reference	Source	Link
Helix DNA Server RTSP Buffer Overflow - Advisories - Secunia	SECUNIA	secunia.com
labs.musecurity.com/wp-content/uploads/2007/08/mu-200708-01.txt	MISC	labs.musecurity.
Helix DNA Server Heap Corruption Vulnerability - CXSecurity.com	SREASON	securityreason.c
'[Full-disclosure] [MU-200708-01] Helix DNA Server Heap Corruption' - MARC	FULLDISC	marc.info

RealNetworks Helix DNA Server RTSP Command Remote Heap Buffer Overflow Vulnerability	BID	www.securityfoc
Helix DNA Server RTSP Require Header Bug Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.securitytrac
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**