

Potential Server Exploit Vulnerability - Update

March 21, 2007

A buffer overflow can occur when the Helix Server processes a data packet containing a modified RTSP "describe" request. The vulnerability causes the Helix Server to crash and may allow an unauthenticated remote attacker to gain root privileges to the server, although no such cases have been reported.

Impacted Products and Versions:

Helix Server Version 11.1.2.

Helix Mobile Server Version 11.1.2.

The Fix:

Version 11.1.3 of the Helix Server and the Helix Mobile Server and have been updated to check for these modified data packets and handle them appropriately.

SOLUTION:

The the vulnerability is resolved on the following platforms by installing Version 11.1.3 of the Helix Server and the Helix Mobile Server. This only pertains to supported versions of the platforms listed below. The updated version will be available on your [RealNetworks PAM site](#) after 11:59 pm PST, on March 21, 2007.

- Linux
- Sun Solaris
- Windows

ACKNOWLEDGMENT:

RealNetworks thanks Evgeny Legerov from GLEG Ltd (<http://gleg.net/index.shtml>) for reporting this vulnerability.

WARRANTY:

While RealNetworks endeavors to provide you with the highest quality products and services, we cannot guarantee and do not warrant that the operation of any RealNetworks product will be error-free, uninterrupted or secure. See your original license agreement for details of our limited warranty or warranty disclaimer.