Helix Server RTSP Buffer Overflow Vulnerability

June 19, 2007

The vulnerability is caused due to a boundary error when processing RTSP commands. The vulnerable code is triggered with the use of an RTSP command with multiple 'Require' headers. After receiving a “Play” request from client, the server validates the request and if there are any un-supported values in any of the common headers, it will send response back to client by appending all un-supported values to the unsupported column. But the buffer allocated to send un-supported value is capable of holding only one un-supported value.

Impacted Products and Versions:

Helix Server Version 11.x
Helix Mobile Server Version 11.x

The Fix:

Version 11.1.4 of the Helix Server and the Helix Mobile Server have been updated to ensure that sending multiple “Require” headers will not cause the server to terminate abnormally.

SOLUTION:

The vulnerability is resolved on the following platforms by installing Version 11.1.4 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 June 19, 2007.

- Red Hat Enterprise Linux 4
- Sun Solaris 8/9
- Windows 2003

ACKNOWLEDGMENT:

RealNetworks would like to thank Gavin Heer from Mu Security (http://musecurity.com) for reporting this vulnerability.