



# MEDIA ALERT

**Corporate Contact:**

Peter Benedict  
Dir. Media and Analyst Relations  
RADVISION  
Tel: 201-689-6311  
[pr@radvision.com](mailto:pr@radvision.com)

## **RADVISION H.323 CURRENT PRODUCTS PROVIDE PROTECTION AGAINST RECENTLY ANNOUNCED VOICE AND VIDEO OVER IP VULNERABILITY**

*All Currently Shipping Videoconferencing and Developer Toolkit Products  
Are Invulnerable to Denial of Service Attacks*

**GLEN ROCK, New Jersey, January 16, 2004** -- In response to recent uncertainty in the market about the vulnerability of certain voice and video over IP solutions based on the H.323 protocol, **RADVISION (Nasdaq: RVSN)** today announced that its current line of products being sold have been tested to be immune to the recently publicized H.323 Denial of Service (DoS) vulnerability.

A report recently released by the U.K. National Infrastructure Security Co-ordination Center (NISCC) highlights a number of implementation-specific vulnerabilities in the H.323 Protocol which, if exploited, could allow an attacker to create a Denial of Service (DoS) condition. For more information see:

<http://www.uniras.gov.uk/vuls/2004/006489/h323.htm>

**Videoconferencing Solutions:**

Infrastructure solutions listed below containing the H.323 Protocol that RADVISION currently offers for sale have been tested to be immune to the published vulnerability.

These include the following products:

- MCU version 3.2 and above
- Gateway version 2.01 and above
- ECS version 3.2.2.2 and above

More information on support for earlier versions of RADVISION infrastructure is available by contacting RADVISION customer service through its Web site at: <http://www.radvision.com/NBU/Customer+Support.htm>

**Developer Solutions:**

RADVISION's H.323 developer toolkits, which are used by a significant portion of the VoIP development market, have, since Q4, 2003, included functionality that enables any product developed with this solution to be invulnerable to the threat contained in the NISCC report. This functionality has been generally available in version 4.2 of its developer toolkit. RADVISION has also been supplying patches to provide similar protection for the latest releases of H.323 v4.1 and v4.0 of its developer toolkit. Therefore, voice and video over IP products that are based on these versions have been tested to show they are not vulnerable to the DoS attacks.

RADVISION customers who are part of the RADVISION maintenance and support program should be in contact with RADVISION support engineers to receive the appropriate version 4 (v4.0 latest version patch, v4.1 latest version patch, or v4.2 current release) that is the most suitable for their products. Customers using version 3 and earlier based H.323 products should contact RADVISION customer support to resolve the specific problem they may have with their legacy products. For any questions, customers or developers should contact RADVISION Customer Support on our Web site at: <http://www.radvision.com/TBU/Customer+Support/>

#### **About RADVISION**

RADVISION Ltd. (Nasdaq: RVSN) is the industry's leading provider of high quality, scalable and easy-to-use products and technologies for videoconferencing, video telephony, and the development of converged voice, video and data over IP and 3G networks. For more information please visit our website at [www.radvision.com](http://www.radvision.com)

All trademarks are properties of their respective owners.