

NISCC Vulnerability Advisory 006489/H323

Vulnerability Issues in Implementations of the H.323 Protocol

Summary

During 2002 the University Of Oulu Security Programming Group (OUSPG) discovered a number of implementation specific vulnerabilities in the Simple Network Management Protocol (SNMP). Subsequent to this discovery, NISCC has performed and commissioned further work on identifying implementation specific vulnerabilities in related protocols that are critical to the UK Critical National Infrastructure. One of these protocols is H.225 which is part of the H.323 family and commonly implemented as a component of multimedia applications such as Voice Over IP.

OUSPG has produced a test suite for H.225 and employed it to validate their findings against a number of products from different vendors. The test results have been confirmed by testing performed by NISCC and the affected vendors contacted with the test results.

The advisory can be viewed on-line at

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

RADVISION's viaIP product line is invulnerable to the H.323 vulnerability test. All current shipping versions of the product line elements (including the MCU, GW and ECS products) are immune to the test. The respective version numbers are:

MCU version 3.2 and above

GW version 2.01 and above

ECS version 3.2.2.2 and above

For more information please contact RADVISION customer support, at:

<http://www.radvision.com/NBU/Customer+Support.htm>.