

26 May 2005



By:

Cisco solves DNS and VoIP flaws

For IP 7902/7905/7912 phones, Unity Express and ACNS devices

A security flaw tracked at the beginning of the week by National Infrastructure Security Co-ordination Centre in the Cisco solutions could lead to the exploitation of routers and Voice Over IP products. Cisco posted yesterday a security patch that blocks Denial-of-Service attacks. The systems that could have launched such attacks received first a specially modified DNS package. The flaw allows connections with an IP network through the DNS IP assigning protocol. The attacker modifies the compressed zone with invalid information, generating in this way processing errors when the identification data is received. After the attack succeeds, the devices involved could suffer blockages or malfunctions, resulting in a Denial-of-Service situation. Cisco has announced that the products affected by this flaw are DNS clients, among which IP 7902/7905/7912 phones, and Unity Express and ACNS devices. Moreover, ATA (Analog Telephone Adapter) 186/188 versions and the 4400 router series are also targeted by this exploit. Because a lot of retailers include support for their products, it's likely that they might have already published security solutions that annihilate this flaw. That is why NISCC didn't rate it as critical flaw and recommended companies to contact their retailers.